

**Service  
Manual**

# hp StorageWorks Director 2/64

**Product Version:** FW v06.xx/HAFM SW v08.02.00

Fourth Edition (July 2004)

**Part Number:** AA-RS2ED-TE

This guide provides procedures for servicing the HP StorageWorks Director 2/64.



© Copyright 2001–2004 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Director 2/64 Service Manual  
Fourth Edition (July 2004)  
Part Number: AA-RS2ED-TE

# Contents

<b>About this Guide</b>	<b>11</b>
Overview	12
Intended Audience	12
Related Documentation	12
Conventions	13
Document Conventions	13
Text Symbols	13
Equipment Symbols	14
Rack Stability	16
Getting Help	17
HP Technical Support	17
HP Storage Web Site	17
HP Authorized Reseller	17
<b>1 General Information</b>	<b>19</b>
Director Description	20
Maintenance Approach	21
Front View	22
Rear View	23
Software Diagnostic Features	24
HAFM and Element Manager Diagnostics	24
HAFM Services Application	25
Event Table	26
Status Line	27
Embedded Web Server Diagnostics	27
SNMP Trap Message Support	29
E-Mail and Call-Home Support	30

Tools and Test Equipment . . . . .	30
Tools Supplied with the Director . . . . .	30
Tools Supplied by Service Personnel . . . . .	32
Additional Information . . . . .	33
<b>2 Diagnostics . . . . .</b>	<b>35</b>
Maintenance Analysis Procedures . . . . .	36
Factory Defaults . . . . .	36
Quick Start . . . . .	37
MAP 0000: Start MAP . . . . .	46
MAP 0100: Power Distribution Analysis . . . . .	71
MAP 0200: POST Failure Analysis . . . . .	81
MAP 0300: HAFM Appliance Software Problem Determination . . . . .	87
MAP 0400: Loss of HAFM or Web Browser PC Communication . . . . .	95
MAP 0500: FRU Failure Analysis . . . . .	110
MAP 0600: UPM Card Failure and Link Incident Analysis . . . . .	118
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination . . . . .	141
MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination . . . . .	157
<b>3 Repair Information . . . . .</b>	<b>165</b>
Factory Defaults . . . . .	166
Procedural Notes . . . . .	166
Using Log Information . . . . .	167
Viewing Logs . . . . .	169
Exporting Log Data . . . . .	170
Obtaining Port Diagnostic Information . . . . .	170
UPM Card LEDs . . . . .	171
HAFM Appliance . . . . .	173
Viewing the Port List View . . . . .	173
Viewing the Performance View . . . . .	175
Viewing Port Properties . . . . .	179
Viewing Port Technology . . . . .	182
EWS Interface . . . . .	182
Viewing the Port List Page . . . . .	183
Viewing the Port Stats Page . . . . .	184
Viewing the Port Properties Page . . . . .	187

---

Performing Loopback Tests . . . . .	188
Internal Loopback Test . . . . .	189
External Loopback Test . . . . .	192
Channel Wrap Test (FICON) . . . . .	195
Swapping Ports (FICON) . . . . .	196
Collecting Maintenance Data . . . . .	197
Clean Fiber Optic Components . . . . .	199
Power-On Procedure . . . . .	200
Power-Off Procedure . . . . .	201
IML, IPL, or Reset the Director . . . . .	202
IML the Director from the CTP Front Panel . . . . .	203
IPL the Director from the HAFM Appliance . . . . .	203
Reset the Director from the CTP Front Panel . . . . .	204
Set the Director Online or Offline . . . . .	205
Set Online State . . . . .	205
Set Offline State . . . . .	206
Block and Unblock Ports . . . . .	207
Block a Port . . . . .	207
Block a UPM Card . . . . .	208
Unblock a Port . . . . .	209
Unblock a UPM Card . . . . .	209
Manage Firmware Versions . . . . .	211
Determine a Director Firmware Version . . . . .	211
Add a Firmware Version . . . . .	212
Modify a Firmware Version Description . . . . .	214
Delete a Firmware Version . . . . .	215
Download a Firmware Version to a Director . . . . .	215
Manage Configuration Data . . . . .	218
Back up the Configuration . . . . .	218
Restore the Configuration . . . . .	219
Reset Configuration Data . . . . .	220
Install or Upgrade Software . . . . .	223
<b>4 FRU Removal and Replacement . . . . .</b>	<b>227</b>
Factory Defaults . . . . .	228
Procedural Notes . . . . .	228
Remove and Replace FRUs . . . . .	229
ESD Information . . . . .	229
Concurrent FRUs . . . . .	230

Non-Concurrent FRUs . . . . .	231
RRP: Redundant CTP2 Card . . . . .	231
Tools Required . . . . .	232
Removing a Redundant CTP2 Card . . . . .	232
Replacing a Redundant CTP2 card . . . . .	233
RRP: UPM Card. . . . .	236
Tools Required . . . . .	236
Removing a UPM Card . . . . .	236
Replacing a UPM Card . . . . .	239
RRP: SFP Optical Transceiver. . . . .	241
Tools Required . . . . .	241
Removing an SFP Optical Transceiver . . . . .	241
Replacing an SFP Optical Transceiver . . . . .	242
RRP: UPM Filler Blank . . . . .	244
Tools Required . . . . .	244
Removing a UPM Filler Blank . . . . .	244
Replacing a UPM Filler Blank . . . . .	245
RRP: Redundant Power Supply . . . . .	245
Tools Required . . . . .	245
Removing a Redundant Power Supply . . . . .	245
Replacing a Redundant Power Supply . . . . .	246
RRP: Redundant SBAR Assembly . . . . .	248
Tools Required . . . . .	248
Removing a Redundant SBAR Assembly . . . . .	248
Replacing a Redundant SBAR Assembly . . . . .	250
RRP: Redundant Fan Module . . . . .	252
Tools Required . . . . .	252
Removing a Redundant Fan Module . . . . .	252
Replacing a Redundant Fan Module . . . . .	253
RRP: Power Module Assembly . . . . .	255
Tools Required . . . . .	255
Removing a Power Module Assembly . . . . .	255
Replacing a Power Module Assembly . . . . .	256
RRP: Backplane . . . . .	258
Tools Required . . . . .	258
Removing a Backplane . . . . .	258
Replacing a Backplane . . . . .	261

<b>5</b>	<b>Illustrated Parts Breakdown. . . . .</b>	<b>265</b>
	Front-Accessible FRUs. . . . .	266
	Rear-Accessible FRUs . . . . .	268
	Miscellaneous Parts . . . . .	270
<b>A</b>	<b>Information and Error Messages . . . . .</b>	<b>271</b>
	HAFM Application Messages . . . . .	272
	Element Manager Messages . . . . .	292
<b>B</b>	<b>Event Code Tables. . . . .</b>	<b>319</b>
	System Events (000 through 199). . . . .	321
	Power Supply Events (200 through 299) . . . . .	343
	Fan Module Events (300 through 399). . . . .	347
	CTP2 Card Events (400 through 499) . . . . .	354
	UPM Card Events (500 through 599). . . . .	369
	SBAR Assembly Events (600 through 699). . . . .	382
	Thermal Events (800 through 899). . . . .	387
	<b>Index . . . . .</b>	<b>393</b>
	<b>Figures</b>	
1	Director FRUs (front access) . . . . .	22
2	Director FRUs (rear access). . . . .	23
3	HAFM Services window . . . . .	26
4	Torque tool and hex adapter. . . . .	30
5	SFP fiber optic loopback plug . . . . .	31
6	Fiber optic protective plug . . . . .	31
7	Null modem cable . . . . .	32
8	LCD panel during boot sequence. . . . .	48
9	HAFM 8 Log In dialog box . . . . .	49
10	View All - HAFM 8 window . . . . .	50
11	Port Properties dialog box . . . . .	56
12	Link Incident Log. . . . .	57
13	Event Log. . . . .	58
14	View panel . . . . .	63
15	View Port Properties panel. . . . .	66
16	View FRU Properties panel . . . . .	68
17	Monitor Log panel . . . . .	70
18	Windows Security dialog box . . . . .	87

19	Task Manager dialog box, Applications tab . . . . .	88
20	Dr. Watson for Windows dialog box . . . . .	92
21	Ethernet Hubs, Daisy-Chained. . . . .	99
22	LCD panel (LAN 2 IP address) . . . . .	102
23	Discover Setup dialog box . . . . .	105
24	Editing Domain Information dialog box . . . . .	106
25	Domain Information dialog box (IP Address page). . . . .	106
26	HAFM message dialog box . . . . .	107
27	UPM card diagram (OSI). . . . .	121
28	UPM card diagram (FICON) . . . . .	121
29	Fabric Parameters dialog box. . . . .	129
30	Switch Binding - State Change dialog box . . . . .	131
31	Fabric Binding dialog box . . . . .	132
32	Switch Binding - Membership List dialog box . . . . .	133
33	Clear Link Incident Alert(s) dialog box. . . . .	135
34	UPM card diagram (OSI). . . . .	140
35	UPM card diagram (FICON) . . . . .	140
36	Configure Switch Parameters dialog box. . . . .	148
37	Zoning dialog box (Zone Library tab) . . . . .	149
38	Zoning dialog box (Active Zone Set tab). . . . .	150
39	View Logs dialog box . . . . .	169
40	Port List View . . . . .	173
41	Performance View . . . . .	175
42	Port Properties dialog box . . . . .	179
43	Port Technology dialog box. . . . .	182
44	Monitor panel (Port List page). . . . .	183
45	Monitor panel (Port Stats page). . . . .	184
46	View panel (Port Properties page). . . . .	187
47	Port Diagnostics dialog box . . . . .	190
48	Save Data Collection dialog box . . . . .	197
49	Data Collection dialog box. . . . .	198
50	Clean fiber optic components. . . . .	199
51	Information dialog box. . . . .	203
52	Set Online State dialog box (offline) . . . . .	205
53	Set Online State dialog box (online) . . . . .	206
54	Blocking Port warning box . . . . .	207
55	Block All Ports dialog box. . . . .	208
56	Unblocking Port warning box . . . . .	209



57 Unblock All Ports dialog box . . . . .	210
58 Firmware Library dialog box . . . . .	211
59 New Firmware Version dialog box . . . . .	213
60 New Firmware Description dialog box . . . . .	213
61 Modify Firmware Description dialog box . . . . .	214
62 Send Firmware dialog box . . . . .	216
63 Send Firmware Complete dialog box . . . . .	217
64 Backup and Restore Configuration dialog box . . . . .	218
65 Backup Complete dialog box . . . . .	219
66 Warning dialog box . . . . .	219
67 Reset Configuration dialog box . . . . .	220
68 Discover Setup dialog box . . . . .	221
69 Domain Information dialog box . . . . .	221
70 Run dialog box . . . . .	224
71 InstallAnywhere dialog box (Introduction) . . . . .	224
72 ESD grounding point (front) . . . . .	229
73 ESD grounding point (rear) . . . . .	230
74 CTP2 card removal and replacement . . . . .	233
75 UPM card removal and replacement . . . . .	238
76 SFP optical transceiver removal and replacement . . . . .	242
77 UPM filler blank removal and replacement . . . . .	244
78 Redundant power supply removal and replacement . . . . .	246
79 SBAR assembly removal and replacement . . . . .	249
80 Fan module removal and replacement . . . . .	253
81 Power module assembly removal and replacement . . . . .	256
82 Backplane removal and replacement . . . . .	260
83 Front-accessible FRUs . . . . .	266
84 Rear-accessible FRUs (part 1) . . . . .	268
85 Rear-accessible FRUs (part 2) . . . . .	269

## Tables

1 Document Conventions . . . . .	13
2 HAFM Services Status Symbols . . . . .	27
3 Factory-set Defaults . . . . .	36
4 MAP Summary . . . . .	37
5 Event Codes and Corresponding Maintenance Action . . . . .	37
6 MAP 0100: Event Codes . . . . .	72
7 MAP 0200: Event Codes . . . . .	82

8	Byte 0 FRU Codes . . . . .	82
9	MAP 0400: Event Codes . . . . .	96
10	MAP 0400: Error Messages and Actions . . . . .	98
11	MAP 0500: Event Codes . . . . .	110
12	MAP 0600: Event Codes . . . . .	119
13	MAP 0600: Port Operational and LED States . . . . .	123
14	MAP 0600: Invalid Attachment Reasons and Actions . . . . .	127
15	MAP 0600: Port Operational States and Actions . . . . .	139
16	MAP 0700: Event Codes . . . . .	141
17	MAP 0700: Segmentation Reasons and Actions . . . . .	143
18	MAP 0700: Byte 4, Segmentation Reasons . . . . .	146
19	Bytes 8 through 11 Failure Reasons and Actions . . . . .	154
20	MAP 0700: Segmentation Reasons and Actions . . . . .	156
21	Factory-set Defaults . . . . .	166
22	Port Operational States . . . . .	171
23	Invalid Attachment Messages and Explanations . . . . .	180
24	Factory-set Defaults . . . . .	228
25	Concurrent FRU Names and ESD Requirements . . . . .	230
26	Non-Concurrent FRU Names and ESD Precautions . . . . .	231
27	Front-Accessible FRU Parts List . . . . .	266
28	Rear-Accessible FRU Parts List (Part 1) . . . . .	268
29	Rear-Accessible FRU Parts List (Part 2) . . . . .	269
30	Miscellaneous Parts . . . . .	270
31	HAFM Messages . . . . .	272
32	Element Manager Messages . . . . .	292

## About this Guide

This guide describes the service procedures for the HP StorageWorks Director 2/64.

“About This Guide” topics include:

- [Overview](#), page 12
- [Conventions](#), page 13
- [Rack Stability](#), page 16
- [Getting Help](#), page 17

## Overview

This section covers the following topics:

- [Intended Audience](#)
- [Related Documentation](#)

## Intended Audience

This publication is intended for service personnel, and any individuals who monitor, configure, and repair the Director 2/64.

## Related Documentation

For a list of corresponding documentation included with this product, see the Related Documents section of the *HP StorageWorks Director Release Notes*.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks web site:

<http://h18006.www1.hp.com/storage/saninfrastructure.html>

For information about Fibre Channel standards, visit the Fibre Channel Industry Association web site, located at <http://www.fibrechannel.org>.

## Conventions

Conventions consist of the following:

- [Document Conventions](#)
- [Text Symbols](#)
- [Equipment Symbols](#)

## Document Conventions

This document follows the conventions in [Table 1](#).

**Table 1: Document Conventions**

Convention	Element
Blue text: <a href="#">Figure 1</a>	Cross-reference links
<b>Bold</b>	Menu items, buttons, and key, tab, and box names
<i>Italics</i>	Text emphasis and document titles in body text
Monospace font	User input, commands, code, file and directory names, and system responses (output and messages)
<i>Monospace, italic font</i>	Command-line and code variables
Blue underlined sans serif font text ( <a href="http://www.hp.com">http://www.hp.com</a> )	Web site addresses

## Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:



**WARNING:** Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.



**Caution:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

---

**Tip:** Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

---

---

**Note:** Text set off in this manner presents commentary, sidelights, or interesting points of information.

---

## Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:



Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

**WARNING:** To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

---



Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

**WARNING:** To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

---



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

**WARNING:** To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

---



Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

**WARNING:** To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.



Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

**WARNING:** To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

## Rack Stability

Rack stability protects personnel and equipment.



**WARNING:** To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
  - The full weight of the rack rests on the leveling jacks.
  - In single rack installations, the stabilizing feet are attached to the rack.
  - In multiple rack installations, the racks are coupled.
  - Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.
-



## Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: <http://www.hp.com>.

## HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: <http://www.hp.com/support/>. From this web site, select the country of origin.

---

**Note:** For continuous quality improvement, calls may be recorded or monitored.

---

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

## HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this web site, select the appropriate product or solution.

## HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers:  
<http://www.hp.com>.
-



# General Information

## 1

The HP StorageWorks Director 2/64 provides dynamic switched connections between Fibre Channel servers and devices in a storage area network (SAN) environment. SANs introduce the concept of server-to-device networking and multi-switch fabrics, eliminate requirements for dedicated connections, and enable the enterprise to become data-centric.

A SAN provides speed, high capacity, and flexibility for the enterprise, and is primarily based upon Fibre Channel architecture. The Director 2/64 implements Fibre Channel technology that provides scalable bandwidth (2.125 gigabits per second), redundant switched data paths, and long transmission distances (up to 35 kilometers with extended reach optical transceivers, or 100 kilometers with repeaters).

This chapter describes:

- [Director Description](#), page 20
- [Maintenance Approach](#), page 21
- [Software Diagnostic Features](#), page 24
- [Tools and Test Equipment](#), page 30
- [Additional Information](#), page 33

## Director Description

The Director 2/64 is a second-generation, 32-port product (expandable to 64 ports) that provides dynamic switched connections between Fibre Channel servers and devices in a SAN environment. Directors (from one to four) can be configured to order in an HP-supplied equipment rack, which can provide up to 256 ports in a single cabinet.

Directors are managed and controlled through a HAFM appliance supplied by HP with the *HAFM* application and Director 2/64 Element Manager installed. The HAFM appliance is a rack-mount server that provides a central point of control for up to 48 directors and/or edge switches. Multiple directors and the HAFM appliance communicate through the customer's local area network (LAN).

The director provides dynamic switched connections for servers and devices, supports mainframe and Open-Systems Interconnection (OSI) computing environments, and provides data transmission and flow control between device node ports (N\_Ports), as dictated by the *Fibre Channel Physical and Signaling Interface* (FC-PH 4.3). Through interswitch links (ISLs), the director can also connect to one or more additional directors or switches to form a Fibre Channel multi-switch fabric.

## Maintenance Approach

Whenever possible, the director maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the director, attached devices, or associated applications. Director fault isolation begins when one or more of the following occur:

- System event information displays at the attached *HAFM* application, a remote workstation communicating with the HAFM appliance or the Embedded Web Server (EWS) interface.
- LEDs on the director front bezel or FRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Notification of a significant system event is received at a designated support center through an e-mail message or the call-home feature.

System events can be related to one of the following occurrences:

- Director or HAFM appliance failure (hardware or software).
- Ethernet LAN communication failure between the director and HAFM appliance.
- Link failure between a port and attached device.
- ISL failure or segmentation of an E\_Port.

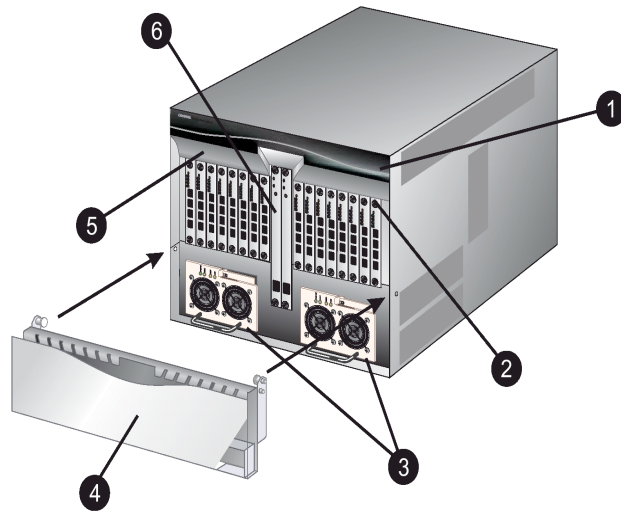
Fault isolation and service procedures vary, depending on the system event information provided. Fault isolation and related service information is provided through maintenance analysis procedures (MAPs) documented in “[Diagnostics](#)” on page 35.

MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system event information, isolate a director failure to a single FRU, remove and replace the failed FRU, and verify director operation.

The fault isolation process normally begins with “[MAP 0000: Start MAP](#)” on page 46. When a fault occurs, ensure that the correct director is selected for service (if the HAFM appliance manages multiple directors or other HP products) by enabling unit beaconing at the failed director. The amber system error LED on the director front bezel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into the MAP steps.

## Front View

Figure 1 displays FRUs accessible from the front of the director.



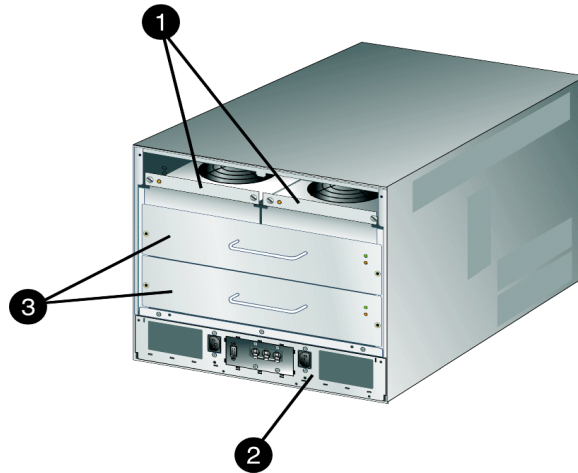
SHR-2272

- |   |  |
|---|--|
| ❶ Power and system error light-emitting diodes (LEDs) | ❹ Front bezel                                |
| ❷ Up to 16 universal port module (UPM) cards          | ❺ Redundant control processor 2 (CTP2) cards |
| ❸ Redundant power supplies                            |  |

**Figure 1: Director FRUs (front access)**

## Rear View

Figure 2 displays FRUs accessible from the rear of the director.



SHR-2312

- ❶ Redundant fan modules
- ❷ Power module assembly with AC power switch
- ❸ Redundant serial crossbar (SBAR) assemblies

**Figure 2: Director FRUs (rear access)**

## Software Diagnostic Features

The director provides the following diagnostic software features that aid in fault isolation and repair of problems:

- On-board diagnostic and monitoring circuits that continuously report FRU status to the *HAFM* application and the Element Manager. The HAFM and Element Manager provide system alerts and logs that display failure and diagnostic information at the HAFM appliance or a remote workstation communicating with the HAFM appliance.
- The *HAFM* application that runs as a Windows® 2000 service and provides an additional user interface to display director operational status.
- The Embedded Web Server interface that provides Internet access to isolate problems for a single director.
- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to as many as 12 authorized management workstations.
- E-mail messages or call-home reports that provide automatic notification of significant system events to designated support personnel or administrators.

## HAFM and Element Manager Diagnostics

---

**Note:** HAFM and Element Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed, and the fields may contain data that does not match the data seen on your system.

---

The *HAFM* application and the Element Manager provide a Java-based GUI to manage, monitor, and isolate problems for multiple directors and multi-switch fabrics.

The *HAFM* application opens automatically when the HAFM appliance is powered on, and the default display is the View All - HAFM 8. Managed products (including directors) display as icons at the top of the window.



The left panel of this view is the product list, which is an expandable list of the fabrics, the products in the fabrics, and the nodes connected to the products. The Physical Map displays graphical fabric elements and ISLs for a multi-switch fabric. The graphical representation of the fabric emulates the configuration and operational status of the corresponding real fabric. Note that a single director without ISLs is still considered a fabric.

Double-click a director icon to open the Element Manager. The Element Manager provides a Java-based GUI to manage, monitor, and isolate problems for a specific director. It operates locally on the HAFM appliance, or through an Ethernet LAN connection from a remote user workstation.

When the Element Manager opens, the default display is the Hardware View. A Director 2/64 Status table and a graphical representation of the director hardware (front and rear) display.

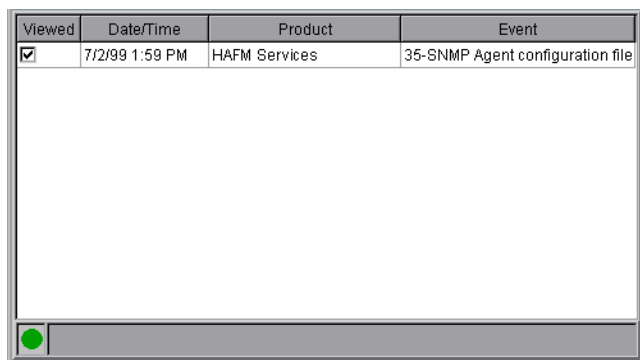
- For a description of the Element Manager, refer to the *HP StorageWorks Director Element Manager User Guide*.
- For a description of the *HAFM* application, refer to the *HP StorageWorks HA-Fabric Manager User Guide*.

## HAFM Services Application

The HP StorageWorks *HAFM Services* application provides a central control point and server-side functionality (in a client-server environment). The application runs as a Windows 2000 service and starts automatically when the HAFM appliance is powered on.

The user interface consists of the HAFM Services window ([Figure 3](#) on page 26), which provides *HAFM* application status and diagnostic information. The HAFM Services window consists of:

- An event table that displays *HAFM* application events that occurred since the *HAFM* application was started.
- A status line at the bottom of the panel that provides a status indicator and message area.



Viewed	Date/Time	Product	Event
<input checked="" type="checkbox"/>	7/2/99 1:59 PM	HAFM Services	35-SNMP Agent configuration file

**Figure 3: HAFM Services window**

## Event Table

The event table displays the last ten events that occurred since the *HAFM* application was started. Events that occurred during a prior instance of the application do not display. If a new event occurs while ten events display, the oldest event is discarded. A deeper event history is maintained in the form of a log file viewed through the *HAFM* application.

The events are internal error conditions detected by the *HAFM* application, and are not related to product-specific events reported by a director. Events typically relate to HAFM audit log and file corruption, invalid product definition and firmware files, missing product services class, or missing version information.

The event table contains the following columns:

- **Viewed**—This column provides a check box associated with each event. Each check box allows service personnel to mark an event as viewed (acknowledged with appropriate action taken).
- **Date/Time**—The date and time the event was reported to the HAFM appliance.
- **Product**—The product associated with the event. Some events are associated with the *HAFM* application, while others are associated with a specific instance of the Element Manager. In the latter case, the product (Director 2/64) and configured name (or IP address) associated with the instance are displayed.
- **Event**—The numeric event code and a brief description of the event.





## Status Line

The status line provides a status indicator and message area. HAFM status symbols are explained in [Table 2](#).

The *HAFM* application icon (upper left corner of the window) is dynamic and matches the status indicator. This feature allows users and service personnel to observe the status when the application is minimized to the **Windows 2000** task bar.

The message area briefly displays messages during *HAFM* application startup to indicate the progress of startup activities.

**Table 2: HAFM Services Status Symbols**

Alert Symbol	Meaning
Blank 	The status indicator is blank during <i>HAFM</i> application initialization.
Green circle 	All events are viewed (acknowledged with appropriate action taken).
Yellow triangle 	One or more nonfatal events have not been viewed.
Red diamond (with yellow background) 	A fatal error occurred.

## Embedded Web Server Diagnostics

If HAFM appliance access is not available, the Embedded Web Server interface provides a GUI accessed through the Ethernet (locally or remotely) to manage, monitor, and isolate problems for a single director. This interface does not replace nor offer the full management capability of the HAFM and Element Manager.

The Embedded Web Server interface can be opened from a standard Web browser such as Netscape Navigator Version 4.6 (or higher) or Microsoft® Internet Explorer Version 4.0 (or higher). At the browser, enter the IP address of the director as the Internet uniform resource locator (URL). When prompted at a login screen, enter a username and password. When the interface opens, the default display is the View panel.

Service personnel can perform monitoring, configuration, maintenance and diagnostic functions as follows:

- **View panel**—Quickly inspect and determine the operational status of the director, and inspect director properties and operating parameters, FRU properties, and Fibre Channel port properties.
- **Configure panel**—Configure or change:
  - Director Fibre Channel ports.
  - Director identification, date and time, operating parameters, and network addresses.
  - SNMP trap message recipients.
  - User passwords.
- **Monitor panel**—Inspect and monitor:
  - Fibre Channel ports and port performance statistics.
  - The active zone set.
  - Event Log entries, and clear the system error LED at the director front bezel.
  - Information about attached devices (nodes).
- **Operations panel**—Perform the following operations and maintenance tasks:
  - Enable port beaconing and perform port diagnostics (internal and external loopback tests).
  - Reset Fibre Channel ports.
  - Set the director online state.
  - Upgrade director firmware.

General tasks performed through the Web server interface are very similar in form and function to tasks performed through the HAFM and Element Manager; therefore, they are not documented in this publication. For task information and descriptions, open the online user documentation (Help selection) that supports the interface.

This publication provides instructions for director fault isolation using the Embedded Web Server interface. See “[Diagnostics](#)” on page 35 for the fault isolation tasks.

## SNMP Trap Message Support

Unsolicited SNMP trap messages that indicate director operational state changes or failure conditions can be customer-configured to be transmitted to up to 12 management workstations. If installed on a dedicated Ethernet LAN, the workstations communicate directly with each director. If installed on a customer intranet, workstations communicate with directors through the HAFM appliance.

SNMP data and trap messages are defined in the Fibre Channel FE-MIB definition, a subset of the TCP/IP MIB-II definition (RFC 1213), and a custom, director-specific MIB. Customers can install these MIBs (in standard ASN.1 format) on any SNMP management workstation.

Although SNMP trap messages are typically transmitted to customers only, the messages may be provided to service personnel as initial notification of a director problem or as information included in the fault isolation process. Generic SNMP traps include:

- **coldStart**—Reports that the SNMP agent is reinitializing due to a director reset.
- **warmStart**—Reports that the SNMP agent is reinitializing due to a director IPL.
- **authorizationFailure**—Reports attempted director access by an unauthorized SNMP manager. This trap is configurable and is disabled by default.

Director-specific SNMP traps specified in the custom MIB include Fibre Channel port operational state changes and FRU operational state changes.

If authorized through the Configure SNMP dialog box in the Element Manager, users at SNMP management workstations can modify MIB variables.

- Director modifications performed through SNMP management workstations are recorded in the associated director audit log and are available through the Element Manager. For additional information, refer to the *HP StorageWorks SNMP Reference Guide for Directors and Edge Switches*.

## E-Mail and Call-Home Support

If e-mail notification and call-home support are configured for the director as part of the customer support process, service personnel may be:

- Notified of a director problem by e-mail message, either directly or through a system administrator at the customer site or call center.
- Assigned a service call from call center personnel upon receipt and confirmation of a director call-home event.

## Tools and Test Equipment

This section describes tools and test equipment that may be required to test, service, and verify operation of the director and attached HAFM appliance. These tools are either supplied with the director or must be supplied by service personnel.

### Tools Supplied with the Director

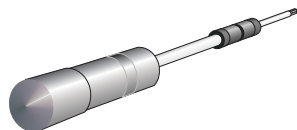
The following tools are supplied with the director. These tools may be required to perform test, service, or verification tasks.

- **Torque tool with hexagonal adapter**—The torque tool with 5/32" hexagonal adapter ([Figure 4](#)) is required to remove and replace director logic cards.



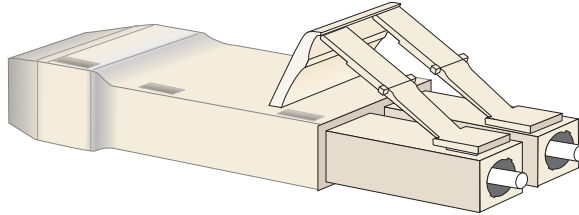
**Caution:** The torque tool supplied with the director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

---



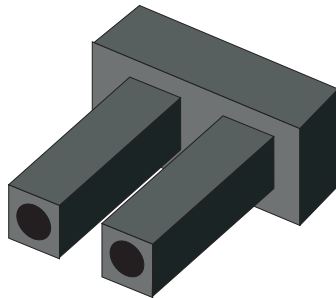
**Figure 4: Torque tool and hex adapter**

- **Fiber optic loopback plug**—An SFP multi-mode (shortwave laser) or single-mode (longwave laser) loopback plug (Figure 5) is required to perform port loopback diagnostic tests. Four multi-mode loopback plugs are shipped with the director. Both plug types are shipped if shortwave laser and longwave laser transceivers are installed.



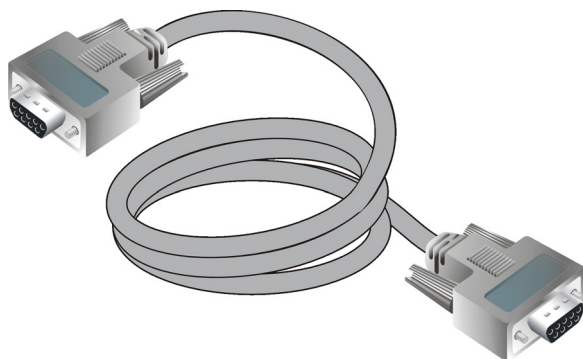
**Figure 5: SFP fiber optic loopback plug**

- **Fiber optic protective plug**—For safety and port transceiver protection, fiber optic protective plugs (Figure 6) must be inserted in all director ports without fiber optic cables attached. The director is shipped with protective plugs installed in all ports.



**Figure 6: Fiber optic protective plug**

- **Null modem cable**—An asynchronous RS-232 null modem cable ([Figure 7](#)) is required to configure director network addresses and acquire Event Log information through the maintenance port. The cable has nine conductors and has DB-9 male and female connectors.



**Figure 7:** Null modem cable

## Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing director maintenance actions. Use of the tools may be required to perform one or more test, service, or verification tasks.

- **Scissors or pocket knife**—A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers**—Screwdrivers are required to remove, replace, adjust or tighten various FRUs, chassis, or cabinet components.
- **T10 Torts<sup>®</sup> tool**—The tool is required to rack-mount the director or to remove, replace, adjust, or tighten various chassis or cabinet components.
- **Electrostatic discharge (ESD) grounding cable with attached wrist strap**—Use of the ESD wrist strap is required when working in and around the director card cage.



- **Maintenance terminal (desktop or notebook PC)**—The PC is required to configure director network addresses and acquire Event Log information through the maintenance port. The PC must have:
  - The Microsoft Windows 98, Windows 2000, Windows XP, or Windows Millennium Edition operating system installed.
  - RS-232 serial communication software installed, such as ProComm Plus or HyperTerminal. HyperTerminal is provided with Windows operating systems.
- **Fiber optic cleaning kit**—The kit contains tools and instructions to clean fiber optic cable, connectors, loopback plugs, and protective plugs.

## Additional Information

The following Director 2/64 documents provide additional information:

- For detailed information about Director 2/64 front and rear panel features, field replaceable units (FRUs), management options and operational features, installation, configuration, and technical specifications, refer to the *HP StorageWorks Director 2/64 Installation Guide*.
- For information on managing the Director 2/64 using the HAFM and Element Manager, refer to the *HP StorageWorks Director Element Manager User Guide*.



# Diagnostics

## 2

This chapter describes diagnostic procedures used by service representatives to fault isolate the Director 2/64 problems or failures to the field-replaceable unit (FRU) level. The chapter describes how to perform the maintenance analysis procedures (MAPs). This chapter includes:

- [Factory Defaults](#), page 36
- [Quick Start](#), page 37
- [MAP 0000: Start MAP](#), page 46
- [MAP 0100: Power Distribution Analysis](#), page 71
- [MAP 0200: POST Failure Analysis](#), page 81
- [MAP 0300: HAFM Appliance Software Problem Determination](#), page 87
- [MAP 0400: Loss of HAFM or Web Browser PC Communication](#), page 95
- [MAP 0500: FRU Failure Analysis](#), page 110
- [MAP 0600: UPM Card Failure and Link Incident Analysis](#), page 118
- [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#), page 141
- [MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination](#), page 157

## Maintenance Analysis Procedures

---

**Note:** HAFM and Element Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed, and the fields may contain data that does not match the data seen on your system.

---

Fault isolation and related service procedures are provided through MAPs. The procedures vary depending on the diagnostic information provided. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system events, isolate a director failure to a single FRU, remove and replace the failed FRU, and verify director operation.

## Factory Defaults

[Table 3](#) lists the defaults for the passwords and IP, subnet, and gateway addresses.

**Table 3: Factory-set Defaults**

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Quick Start

Table 4 lists the MAPs. Fault isolation normally begins at “MAP 0000: Start MAP” on page 46.

**Table 4: MAP Summary**

MAP	Page
MAP 0000: Start MAP	46
MAP 0100: Power Distribution Analysis	71
MAP 0200: POST Failure Analysis	81
MAP 0300: HAFM Appliance Software Problem Determination	87
MAP 0400: Loss of HAFM or Web Browser PC Communication	95
MAP 0500: FRU Failure Analysis	110
MAP 0600: UPM Card Failure and Link Incident Analysis	118
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	141
MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination	157

Table 5 lists the event codes and the corresponding MAPs. It is a quick start, if an event code is readily available.

**Table 5: Event Codes and Corresponding Maintenance Action**

Event Code	Explanation	Action
001	System power-down.	Power on director.
010	Login server unable to synchronize databases.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
011	Login server database invalid.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
020	Name server unable to synchronize databases.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
021	Name server database invalid.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
031	SNMP request received from unauthorized community.	Add community name.
050	HAFM appliance unable to synchronize databases.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
051	HAFM appliance database invalid.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
052	HAFM appliance internal error.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
060	Fabric controller unable to synchronize databases.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
061	Fabric controller database invalid.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
062	Maximum interswitch hop count exceeded.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
063	Remote director or switch has too many ISLs.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
070	E_Port is segmented.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
071	Director is isolated.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
072	E_Port connected to unsupported switch.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
073	Fabric initialization error.	Event data intended for engineering evaluation. Perform data collection procedure (" <a href="#">Collecting Maintenance Data</a> " on page 197) and return backup CD to HP support personnel.
074	ILS frame delivery error threshold exceeded.	Event data intended for engineering evaluation. Perform data collection procedure (" <a href="#">Collecting Maintenance Data</a> " on page 197) and return backup CD to HP support personnel.
080	Unauthorized World-Wide Name.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
081	Invalid attachment.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
090	Database replication time out.	Perform the data collection procedure and return the information to HP for analysis by third-level support personnel.
091	Database replication discontinued.	No action required, unless this event occurs without the backup CTP2 failing or being removed. If so, perform the data collection procedure and return the information to HP for analysis by third-level support personnel.

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
120	Error while processing system management command.	If this event persists, perform data collection procedure (" <a href="#">Collecting Maintenance Data</a> " on <a href="#">page 197</a> ) and return backup CD to HP support personnel.
121	Zone set activation failed—zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
143	Low BB_Credit relieved on an ISL.	No action required.
150	Zone merge failure.	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination</a> .
151	Fabric configuration failure.	If this event persists, perform data collection procedure (" <a href="#">Collecting Maintenance Data</a> " on <a href="#">page 197</a> ) and return backup CD to HP support personnel.
200	Power supply AC voltage failure.	Go to <a href="#">MAP 0100: Power Distribution Analysis</a> .
201	Power supply DC voltage failure.	Go to <a href="#">MAP 0100: Power Distribution Analysis</a> .
202	Power supply thermal failure.	Go to <a href="#">MAP 0100: Power Distribution Analysis</a> .
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.



**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
208	Power supply false shutdown.	Go to <a href="#">MAP 0100: Power Distribution Analysis</a> .
300	Cooling fan propeller failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a>
301	Cooling fan propeller failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
302	Cooling fan propeller failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
303	Cooling fan propeller failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
304	Cooling fan propeller failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
305	Cooling fan propeller failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
320	Fan module removed.	Replace FRU.
321	Fan module installed.	No action required.
400	Power-up diagnostic failure.	Go to <a href="#">MAP 0200: POST Failure Analysis</a> .
410	CTP2 card reset.	No action required.
411	Firmware fault.	Go to <a href="#">MAP 0200: POST Failure Analysis</a> .

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
412	CTP2 watchdog timer reset.	Perform data collection procedure ( <a href="#">“Collecting Maintenance Data” on page 197</a> ) and return backup CD to HP support personnel.
413	Backup CTP2 card POST failure.	Go to <a href="#">MAP 0200: POST Failure Analysis</a> .
414	Backup CTP2 card failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
415	Backup CTP2 card removed.	Replace FRU.
416	Backup CTP2 card installed.	No action required.
417	CTP2 card firmware synchronization initiated.	No action required.
418	User-initiated CTP2 card switchover.	No action required.
420	Backup CTP2 card NV-RAM failure.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
421	Firmware download complete.	No action required.
422	CTP2 firmware synchronization complete.	No action required.
423	CTP2 firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	No action required.
430	Excessive Ethernet transmit errors.	Go to <a href="#">MAP 0400: Loss of HAFM or Web Browser PC Communication</a> .
431	Excessive Ethernet receive errors.	Go to <a href="#">MAP 0400: Loss of HAFM or Web Browser PC Communication</a> .
432	Ethernet adapter reset.	Go to <a href="#">MAP 0400: Loss of HAFM or Web Browser PC Communication</a> .

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
433	Non-recoverable Ethernet fault.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
440	Embedded port hardware failed.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
450	Serial Number mismatch detected.	No action required—Any configured Feature Keys will be cleared, configuration information will be synched with the backplane VPD, and the CTP2 will automatically be IPLed.
451	Switch speed incompatibility detected.	No action required—Switch speed configuration and port speed configuration data will be set to a level that is compatible with the CTP2, and the CTP2 will automatically be IPLed.
452	Backup CTP2 incompatible with configured system settings.	Replace the backup CTP2 with a version of hardware capable of supporting the user-configured settings, or adjust the user settings to be compatible with the backup CTP2, and reseal the backup CTP2.
453	New feature key installed.	No action required.
500	UPM card hot-insertion initiated.	No action required.
501	UPM card recognized.	No action required.
502	UPM card anomaly detected.	No action required.
503	UPM card hot-removal completed.	No action required.

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
504	UPM card failure.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
505	UPM card revision not supported.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
506	Fibre Channel port failure.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
507	Loopback diagnostics port failure.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
508	Fibre Channel port anomaly detected.	No action required.
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
581	Implicit incident.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
582	Bit error threshold exceeded.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
583	Loss of signal or loss of synchronization.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
584	Not operational primitive sequence received.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
585	Primitive sequence timeout.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
586	Invalid primitive sequence received for current link state.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
600	SBAR assembly hot-insertion initiated.	No action required.
601	SBAR assembly recognized.	No action required.
602	SBAR assembly anomaly detected.	No action required.
603	SBAR assembly hot-removal completed.	No action required.
604	SBAR assembly failure.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
605	SBAR assembly revision not supported.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
607	Director contains no operational SBAR assemblies.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
608	User initiated SBAR switch-over.	No action required.
800	High temperature warning (UPM card thermal sensor).	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
801	Critically hot temperature warning (UPM card thermal sensor).	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .
802	UPM card shutdown due to thermal violation.	Go to <a href="#">MAP 0600: UPM Card Failure and Link Incident Analysis</a> .

**Table 5: Event Codes and Corresponding Maintenance Action (Continued)**

Event Code	Explanation	Action
805	High temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
806	Critically hot temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
807	SBAR assembly shutdown due to thermal violation.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
810	High temperature warning (CTP2 card thermal sensor).	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
811	Critically hot temperature warning (CTP2 card thermal sensor).	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
812	CTP2 card shutdown due to thermal violation.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .
850	System shutdown due to CTP2 card thermal violations.	Go to <a href="#">MAP 0500: FRU Failure Analysis</a> .

## MAP 0000: Start MAP

This MAP describes initial fault isolation for the Director 2/64. Fault isolation begins at the HAFM appliance, failed director, Internet-connected personal computer (PC) running the Embedded Web Server interface, or director-attached host.

### 1

Prior to fault isolation, acquire the following information from the customer:

- A system configuration drawing or planning worksheet that includes the HAFM appliance, directors, other HP products, and device connections.
- The location of the HAFM appliance and all directors.
- The internet protocol (IP) address, gateway address, and subnet mask for the director reporting the problem.
- If performing fault isolation using the HAFM appliance:

- The Windows 2000 user name and password. These are required when prompted during any MAP or repair procedure that directs the HAFM appliance to be rebooted.
- The user name, maintenance password, and HAFM appliance name. All are case-sensitive and required when prompted at the HAFM 8 Log In dialog box.
- If performing fault isolation using the Embedded Web Server interface, the director user name and password. Both are case-sensitive and required when prompted at the Username and Password Required dialog box.

**Continue.**

---

## 2

Are you at the HAFM appliance?

**YES            NO**

↓

Go to [step 24](#).

---

## 3

Did the HAFM appliance lock up or crash and:

- Display an application warning or error message, or
- Not display an application warning or error message, or
- Display a Dr. Watson for Windows 2000 dialog box?

**NO            YES**

↓

A HAFM appliance application problem is indicated. Event codes are not recorded. Go to “[MAP 0300: HAFM Appliance Software Problem Determination](#)” on page 87. **Exit MAP.**

---

**4**

Did the HAFM appliance crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

**NO**            **YES**



A HAFM appliance application problem is indicated. Event codes are not recorded. Go to “[MAP 0300: HAFM Appliance Software Problem Determination](#)” on page 87. **Exit MAP.**

---

**5**

Is the *HAFM* application active?

**NO**            **YES**




Go to [step 7](#).

---

**6**

Reboot the HAFM appliance.

1. Click **Start > Shut Down**. The Shut Down Windows dialog box displays.
2. Click **Shut down** on the drop-down list and click **Yes** to power off the HAFM appliance.
3. Wait approximately 30 seconds and press the power () button on the liquid crystal display (LCD) panel to power on the appliance and perform power-on self-test (POST). During POST:
  - a. The green LCD panel illuminates.
  - b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  - c. After a few seconds, the LCD panel displays a message, as shown in [Figure 8](#).

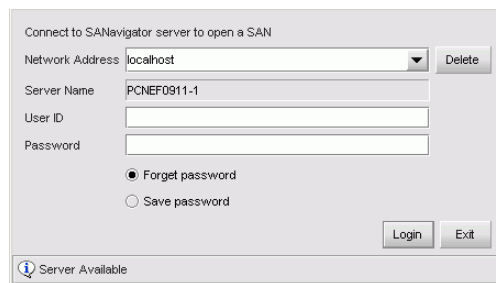


**Boot from LAN?**  
**Press <Enter>**

**Figure 8: LCD panel during boot sequence**



- d. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POST and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - Central processing unit (CPU) temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
4. After successful POST completion, the LCD panel displays a *Welcome!!* message, then continuously cycles through and displays server operational information.
5. After rebooting the server at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. The *HAFM* application starts, and the HAFM 8 Log In dialog box displays, as shown in [Figure 9](#).

The image shows a Windows-style dialog box titled "Connect to SANavigator server to open a SAN". It contains several input fields: "Network Address" with a dropdown menu showing "localhost" and a "Delete" button; "Server Name" with a text field containing "PCNEF0911-1"; "User ID" with an empty text field; and "Password" with an empty text field. Below these fields are two radio buttons: "Forget password" (which is selected) and "Save password". At the bottom right are "Login" and "Exit" buttons. At the bottom left is a status bar with a blue circular icon and the text "Server Available".

**Figure 9: HAFM 8 Log In dialog box**

6. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*.

The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.

If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.

7. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
8. If you want your computer to save the login information, click **Save Password**.
9. Click **Login**. The View All - HAFM 8 window displays, as shown in Figure 10.

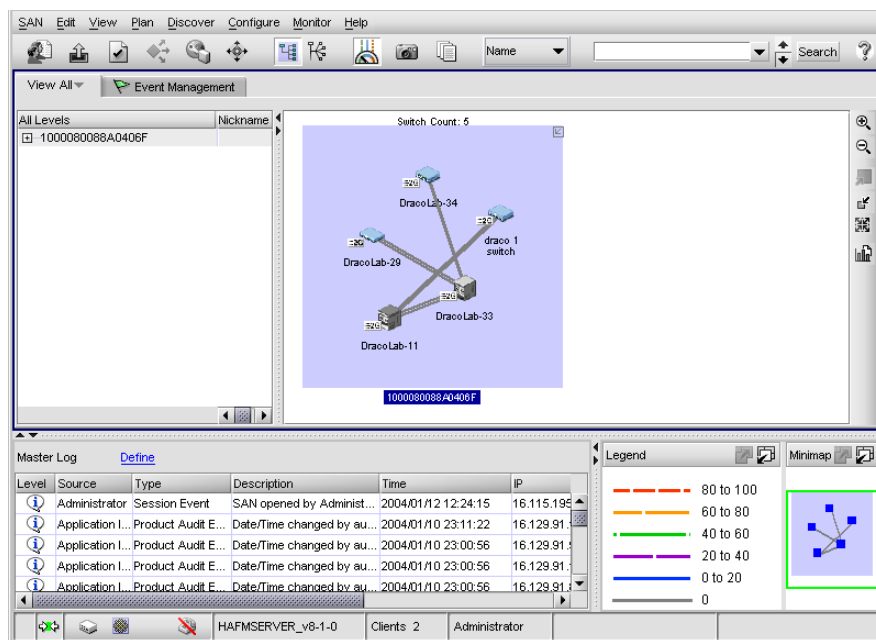


Figure 10: View All - HAFM 8 window

Did the View All - HAFM 8 window display and is the *HAFM* application operational?

**YES**      **NO**



A HAFM appliance hardware problem is indicated. Event codes are not recorded. Go to “[MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination](#)” on page 157. **Exit MAP.**

---

## 7

Inspect the alert indicators of each managed director at the main window physical map or product list. The indicator shows the status of managed directors or the status of the link between the HAFM appliance and managed directors as follows:

- No status symbol indicates that the director is operational.
- A yellow triangle indicates that the director is operating in degraded mode.
- A red diamond indicates that the director is not operational.
- A grey square with yellow exclamation mark indicates that the status of the director is unknown.

Is there a grey square with yellow exclamation mark associated with the icon representing the director reporting the problem?

**YES**      **NO**



Go to [step 11](#).

The grey square indicates the HAFM appliance cannot communicate with the director because:

- The director-to-HAFM appliance Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's control processor (CTP) cards failed.

**Continue.**

---

## 8

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**



A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 9

At the director, inspect the amber LED at the top of each CTP2 card.

Is the amber LED illuminated on both CTP2 cards?

**NO**            **YES**



Failure of both CTP2 cards is indicated. Event codes are not recorded. Go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

## 10

A director-to-HAFM appliance Ethernet link failure is indicated.

Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0400: Loss of HAFM or Web Browser PC Communication](#)” on page 95. **Exit MAP.**

---

## 11

Does a red diamond (failure indicator) display as the background to the icon representing the director reporting the problem?

**YES**            **NO**



Go to [step 14](#).

## 12

Double-click the icon representing the director reporting the problem. The Hardware View displays. At the Hardware View:

- Observe the director Status table is yellow and the director status is **NOT OPERATIONAL**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Do blinking red and yellow diamonds overlay all UPM card graphics?

**NO**                      **YES**



Failure of all installed UPM cards is indicated. **Go to [step 23](#)** to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**

---

## 13

Blinking red and yellow diamonds overlay both serial crossbar (SBAR) assembly graphics or both fan module graphics.

Redundant FRU failures are indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

## 14

Does a yellow triangle (attention indicator) display as the background to the icon representing the director reporting the problem?

**YES**                      **NO**



Go to [step 18](#).

---

## 15

Double-click the icon representing the director reporting the problem. The Hardware View displays. At the Hardware View:

- Verify the Director 2/64 Status table is yellow and the director status is **Minor Failure** or **Redundant Failure**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Does a blinking red and yellow diamond overlay a power supply graphic?

**NO**                      **YES**



A power supply failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 16

Does a blinking red and yellow diamond overlay a UPM card graphic?

**NO**                      **YES**



A UPM card failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**

---

## 17

A blinking red and yellow diamond overlays a control processor (CTP) card, SBAR assembly, or fan module graphic.

An FRU failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

## 18

No colored attention indicator is associated with the icon representing the director reporting the problem. Although the director is operational, a minor problem may exist.

Double-click the icon representing the director reporting the problem. The Hardware View displays. At the Hardware View:

- Inspect CTP2 cards, SBAR assemblies, and fan modules for a yellow triangle that overlays the FRU graphic and indicates FRU beaconing is enabled.
- Inspect UPM cards for a yellow triangle (attention indicator) that overlays the UPM card graphic.

Does a yellow triangle overlay a CTP2 card, SBAR assembly, or fan module graphic?

**YES**            **NO**

↓

Go to [step 20](#).

---

## 19

Beaconing is enabled for the FRU.

1. Consult the customer and next level of support to determine the reason FRU beaconing is enabled.
2. Disable FRU beaconing.
  - a. At the Hardware View, right-click the FRU graphic. A menu displays.
  - b. Click **Enable Beaconing**. The check mark disappears from the box adjacent to the option, and FRU beaconing is disabled.

Was FRU beaconing enabled because an FRU failure or degradation was suspected?

**YES**            **NO**

↓

The director is operational. **Exit MAP.**

Go to [step 22](#).

---

## 20

Does a yellow triangle (attention indicator) overlay a UPM card graphic?

**YES**            **NO**

↓

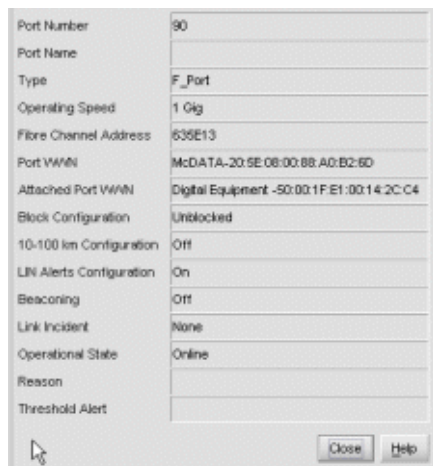
Go to [step 22](#).

---

## 21

Inspect the port state and LED status for all UPM cards with an attention indicator.

1. Double-click the UPM card. The Port Card View displays.
2. Double-click the port graphic with the attention indicator. The Port Properties dialog box displays, as shown in [Figure 11](#).



**Figure 11: Port Properties dialog box**

3. Inspect the **Operational State** field.

Does the **Operational State** field display a **Segmented E\_Port** message?

**NO**                      **YES**



Expansion port (E\_Port) segmentation is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#)” on page 141. **Exit MAP.**

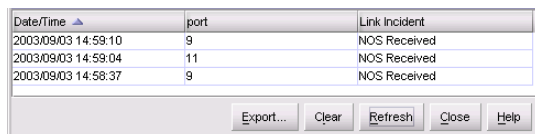
A message displays indicating a link incident problem. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**



## 22

A link incident may have occurred, but the LIN alerts option is not enabled for the port, and the attention indicator does not display.

1. At the Hardware View, click **Logs > Link Incident Log**. The Link Incident Log displays, as shown in [Figure 12](#).



Date/Time	port	Link Incident
2003/09/03 14:59:10	9	NOS Received
2003/09/03 14:59:04	11	NOS Received
2003/09/03 14:58:37	9	NOS Received

**Figure 12: Link Incident Log**

If a link incident occurred, the affected port number is listed with one of the following messages.

Link interface incident-implicit incident.

Link interface incident-bit-error threshold exceeded.

Link failure-loss of signal or loss of synchronization.

Link failure-not-operational primitive sequence (NOS) received.

Link failure-primitive sequence timeout.

Link failure-invalid primitive sequence received for the current link state.

Did one of the listed messages display in the Link Incident Log?

**YES**

**NO**



The director is operational. **Exit MAP.**

A link incident problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**

## 23

Obtain event codes from the director Event Log.

**Note:** If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem has been recovered.

1. At the Hardware View, click **Logs > Event Log**. The Event Log displays, as shown in [Figure 13](#).
2. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).
3. Record all event codes that may relate to the reported problem.

Date/Time	Event	Description	Severity	FRU-Position	Event Data
2003/09/03 14:44:02	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:57	513	SFP optics hot removed	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:43	207	Power supply installed.	INFORMATIONAL	1	
2003/09/03 14:43:30	206	Power supply removed.	INFORMATIONAL	1	
2003/09/03 14:43:21	301	A cooling fan propeller has failed.	FATAL	1	01 00 00 00 0...
2003/09/03 14:43:09	300	A cooling fan propeller has failed.	FATAL	1	00 00 00 00 0...
2003/09/03 14:43:05	200	Power supply AC voltage failure.	FATAL	1	
2003/09/03 14:42:03	203	Power supply AC voltage recovery.	INFORMATIONAL	0	
2003/09/03 14:41:58	200	Power supply AC voltage failure.	FATAL	0	
2003/09/03 14:41:31	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	09 FF FF FF 0...
2003/09/03 14:41:26	513	SFP optics hot removed	INFORMATIONAL	0	09 FF FF FF 0...

**Figure 13: Event Log**

Were one or more event codes found?

**NO**      **YES**



Go to [Table 5](#) on page 37.

Return to the MAP step that sent you here.

## 24

Are you at the director reporting the problem?

**YES**      **NO**



Go to [step 36](#).

---

**25**

Is the power LED (green) at the director front bezel illuminated?

**NO**            **YES**

↓                Go to [step 30](#).

---

**26**

Is the director connected to facility AC power and powered on?

**NO**            **YES**

↓                Go to [step 29](#).

---

**27**

Connect the director to facility AC power and set the power switch (circuit breaker) at the rear of the director to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**

↓                A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 28

Is the power LED (green) at the director front bezel illuminated?

**NO**                      **YES**



Go to [step 30](#).

A faulty power LED is indicated, but director and Fibre Channel port operation is not disrupted. The LED is connected to the circuitry in a fan module, and the module must be removed and replaced (“[RRP: Redundant Fan Module](#)” on page 252). **Exit MAP.**

---

## 29

Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**                      **NO**



A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

A faulty power LED is indicated, but director and Fibre Channel port operation is not disrupted. The LED is connected to the circuitry in a fan module, and the module must be removed and replaced (“[RRP: Redundant Fan Module](#)” on page 252). **Exit MAP.**

---

## 30

Is the system error LED (amber) at the director front bezel blinking?

**YES**                      **NO**



Go to [step 32](#).

---

## 31

Unit beaconing is enabled for the director.

1. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
2. Disable unit beaconing.
  - a. At the Hardware View, right-click the front bezel graphic (away from an FRU). A menu displays.
  - b. Click **Enable Unit Beaconing**. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was unit beaconing enabled because a director failure or degradation was suspected?

**YES**      **NO**

↓      The director is operational. **Exit MAP.**

Go to [step 24](#).

---

## 32

Is the system error LED (amber) at the director front bezel illuminated?

**YES**      **NO**

↓      The director is operational. Verify operation at the HAFM appliance.  
Go to [step 3](#).

---

## 33

Check FRUs (UPM cards, CTP2 cards, SBAR assemblies, power supplies, and fan modules) for failure symptoms.

Is the amber LED at the top of a UPM card illuminated or are any amber LEDs associated with Fibre Channel ports illuminated?

**NO**      **YES**

↓      A UPM card or Fibre Channel port failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118.  
**Exit MAP.**

---

**34**

Is the amber LED on a CTP2 card, SBAR assembly, or fan module illuminated?

**NO**            **YES**



An FRU failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

**35**

Is the green **PWR OK** LED on a power supply extinguished?

**NO**            **YES**



A power supply failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

The director is operational. **Exit MAP.**

---

**36**

Are you at a PC with a Web browser (such as Netscape Navigator or Microsoft Internet Explorer) and an Internet connection to the director reporting the problem?

**YES**            **NO**



Go to [step 53](#).

---

**37**

Is the Web browser PC powered on and communicating with the director through the Internet connection?

**NO**            **YES**



Go to [step 39](#).

---

**38**

Boot the Web browser PC.

1. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop displays.
2. Launch the PC browser application by double-clicking the appropriate icon at the Windows desktop.

3. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the director (obtained in [step 1](#)). The Username And Password Required dialog box displays.
4. Type the user name and password obtained in [step 1](#), and click **OK**. The **Embedded Web Server** interface opens with the View panel displayed, as shown in [Figure 14](#).

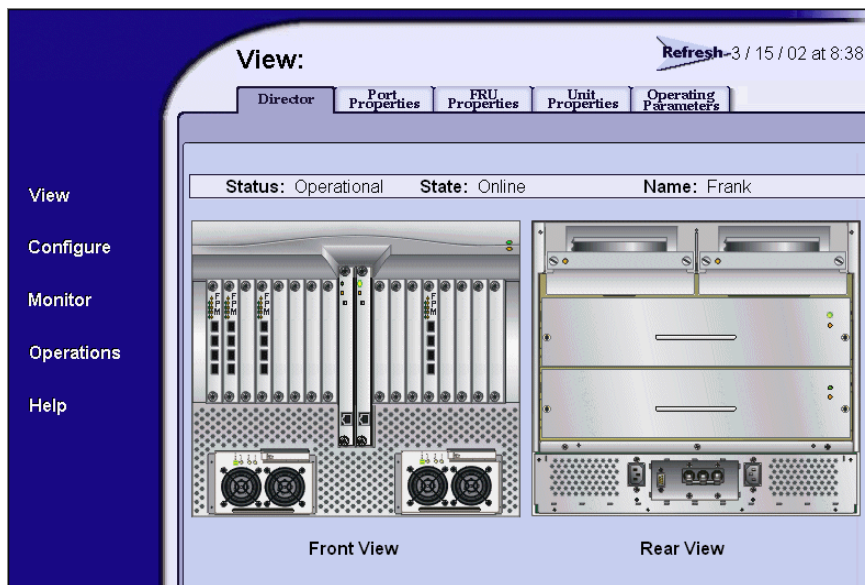


Figure 14: View panel

**Continue.**

**39**

Is the Embedded Web Server interface operational with the View panel displayed?

**NO**

**YES**

↓

Go to [step 44](#).

---

## 40

A Page cannot be found, Unable to locate the server, HTTP 404-file not found, or other similar message displays. The message indicates the Web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**

---

## 41

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**

↓

A power distribution problem is indicated. Go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 42

At the director, inspect the amber LED at the top of each CTP2 card.

Is the amber LED illuminated on both CTP2 cards?

**NO**            **YES**

↓

Failure of both CTP2 cards is indicated. Event codes are not recorded. Go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**



---

**43**

A director-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) is indicated.

1. Wait approximately five minutes, then attempt to log in to the director again.
2. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the director (obtained in [step 1](#)). The Username and Password Required dialog box displays.
3. Type the user name and password obtained in [step 1](#), and click **OK**. If the View panel does not display, wait another five minutes and perform this step again.

Is the Embedded Web Server interface operational with the View panel displayed?

**YES**            **NO**

↓            Perform director fault isolation at the HAFM appliance. Go to [step 3](#).

---

**44**

At the View panel, inspect the **Status** field.

Does the director status indicate **Operational**?

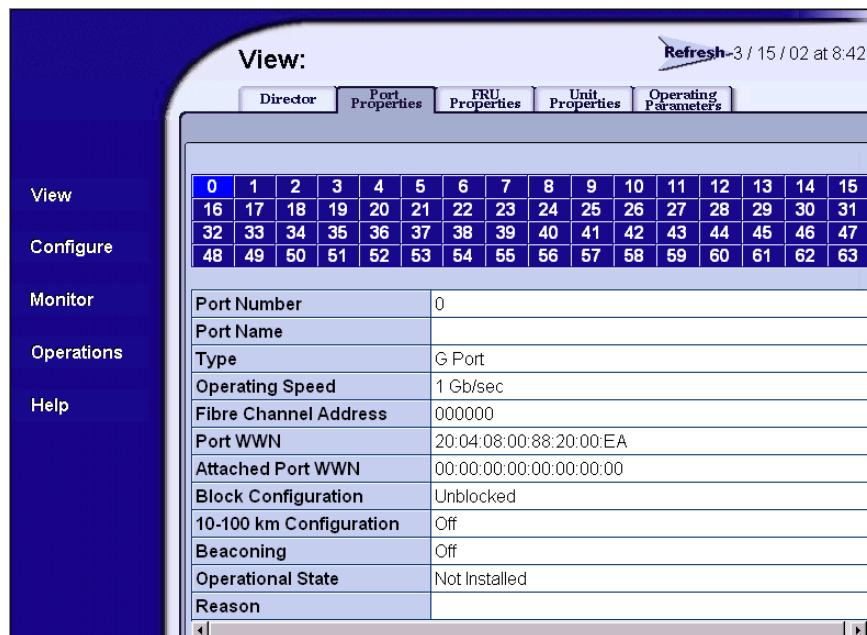
**NO**            **YES**

↓            The director is operational. **Exit MAP.**

## 45

Inspect Fibre Channel port operational states.

1. At the View panel, click the **Port Properties** tab. The **View Port Properties** panel displays, as shown in [Figure 15](#).
2. Inspect the **Beaconing** and **Operational State** fields.



**Figure 15: View Port Properties panel**

Does the **Beaconing** field display an **On** message?

**YES**

**NO**

↓

Go to [step 47](#).

---

## 46

Port beaconing is enabled.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.
2. Disable port beaconing:
  - a. At the View panel, click **Operations** at the left side of the panel. The **Operations** panel opens with the Port Beaconing page displayed.
  - b. Click the **Beaconing State** check box for the port. The check mark disappears from the box and port beaconing is disabled.
  - c. Return to the View panel (**Port Properties** tab).

**Continue.**

---

## 47

At the View panel, does the **Operational State** field display a Segmented message?

**NO**                      **YES**

↓

Port segmentation is indicated. Go to [step 52](#) to obtain event codes. If no event codes are found, go to “[MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#)” on page 141. **Exit MAP.**

---

## 48

At the View panel, does the **Operational State** field display a message indicating a port problem?

**NO**                      **YES**

↓

Go to [step 52](#) to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**

## 49

Repeat [step 45](#) through [step 48](#) for each remaining Fibre Channel port for which a problem is suspected.

Is a problem indicated for any of the ports?

**NO**      **YES**



Go to [step 52](#) to obtain event codes. If no event codes are found, go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**

## 50

Inspect power supply operational states.

- At the View panel, click the **FRU Properties** tab. The **View FRU Properties** panel displays, as shown in [Figure 16](#).

FRU	Position	Status	Part Number	Serial Number
CTP	0	Active	470-000410-361	80341657
CTP	1	Backup	470-000410-361	80322136
SBAR	0	Active	002-002259-100	20460042
SBAR	1	Backup	002-002259-100	81160560
Power	0	Active	721-000042-001	Z59001930
Power	1	Active	721-000042-001	Z59001929
Fan	0	Active		
Fan	1	Active		
Backplane	0	Active	470-000418-202	20430519
Not Installed	0			
Not Installed	1			
Not Installed	2			
Not Installed	3			
GSF1	4	Active	470-000439-004	80430387
Not Installed	5			
Not Installed	6			
Not Installed	7			
Not Installed	8			
Not Installed	9			
Not Installed	10			
Not Installed	11			
GSF1	12	Active	470-000439-004	80430551
Not Installed	13			
GSF1	14	Active	470-000439-004	80430336
GSF1	15	Active	470-000439-004	80430296

**Figure 16: View FRU Properties panel**

2. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a **Failed** message for either power supply?

**NO**                      **YES**



A power supply failure is indicated. Go to [step 52](#) to obtain event codes. If no event codes are found, go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 51

Inspect the **Status** fields for director FRUs, including CTP2 cards, SBAR assemblies, fan modules, and the backplane.

Does the **Status** field display a **Failed** message for any of the FRUs?

**YES**                      **NO**



The director is operational. **Exit MAP.**

An FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

## 52

Obtain event codes from the Embedded Web Server Event Log.

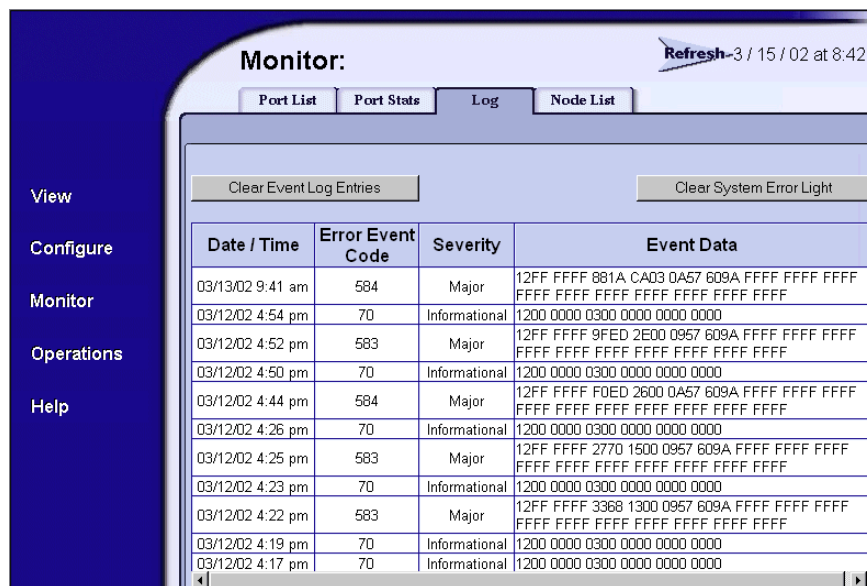
---

**Note:** If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

---

1. At the View panel, click **Monitor** at the left side of the panel. The **Monitor** panel opens with the **Port List** panel displayed.
2. At the **Monitor** panel, click the **Log** tab. The Monitor Log panel displays, as shown in [Figure 17](#) on page 70.
3. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).

4. Record all event codes that may relate to the reported problem.



**Monitor:** Refresh-3 / 15 / 02 at 8:42

Port List Port Stats Log Node List

Clear Event Log Entries Clear System Error Light

Date / Time	Error Event Code	Severity	Event Data
03/13/02 9:41 am	584	Major	12FF FFFF 881A CA03 0A57 609A FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
03/12/02 4:54 pm	70	Informational	1200 0000 0300 0000 0000 0000
03/12/02 4:52 pm	583	Major	12FF FFFF 9FED 2E00 0957 609A FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
03/12/02 4:50 pm	70	Informational	1200 0000 0300 0000 0000 0000
03/12/02 4:44 pm	584	Major	12FF FFFF F0ED 2600 0A57 609A FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
03/12/02 4:26 pm	70	Informational	1200 0000 0300 0000 0000 0000
03/12/02 4:25 pm	583	Major	12FF FFFF 2770 1500 0957 609A FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
03/12/02 4:23 pm	70	Informational	1200 0000 0300 0000 0000 0000
03/12/02 4:22 pm	583	Major	12FF FFFF 3368 1300 0957 609A FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
03/12/02 4:19 pm	70	Informational	1200 0000 0300 0000 0000 0000
03/12/02 4:17 pm	70	Informational	1200 0000 0300 0000 0000 0000

**Figure 17: Monitor Log panel**

Were one or more event codes found?

**NO YES**



Go to [Table 5](#) on page 37.

Return to the MAP step that sent you here.

## 53

You are at the console of an OSI or FICON server attached to the director reporting the problem. If an incident occurs on the Fibre Channel link between the director and server, a link incident record is generated and sent to the server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON).

Was a link incident record generated and sent to the director-attached OSI or FICON server?

**YES NO**



Perform director fault isolation at the HAFM appliance. Go to [step 3](#).

---

## 54

The link incident record provides the attached director port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

**581**—Link interface incident—implicit incident.

**582**—Link interface incident—bit-error threshold exceeded.

**583**—Link failure—loss of signal or loss of synchronization.

**584**—Link failure—not-operational primitive sequence (NOS) received.

**585**—Link failure—primitive sequence timeout.

**586**—Link failure—invalid primitive sequence received for the current link state.

Were one or more event codes found?

**YES**      **NO**



Perform director fault isolation at the HAFM appliance (or customer-supplied server). Go to [step 3](#).

Go to [Table 5](#) on page 37.

## MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the director power distribution system, including defective AC power cords, redundant power supplies, or the power module assembly.

---

### 1

Was an event code **200**, **201**, **202**, or **208** observed at the Director 2/64 Event Log (HAFM appliance) or at the EWS Event Log?

**YES**      **NO**



Go to [step 10](#).

## 2

[Table 6](#) lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

**Table 6: MAP 0100: Event Codes**

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to <a href="#">step 3</a>
201	Power supply DC voltage failure.	Go to <a href="#">step 7</a>
202	Power supply thermal failure.	Go to <a href="#">step 7</a>
208	Power supply false shutdown.	Go to <a href="#">step 8</a>

---

## 3

A redundant power supply is disconnected from facility power, not properly installed, or has failed.

Verify the power supply is connected to facility power.

1. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the director and a facility power receptacle. If not, connect the cord as directed by the customer.
2. Ensure the associated facility circuit breaker is on. If not, ask the customer to set the circuit breaker on.
3. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

**YES**

**NO**

↓

Go to [step 5](#).

---

## 4

Verify redundant power supply operation.

1. Inspect the power supply and ensure the green **PWR OK** LED illuminates and all amber LEDs extinguish.
2. At the Hardware View, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not display.



Is a failure indicated?

**YES**      **NO**

↓              The director is operational. **Exit MAP.**

---

## 5

Ensure the indicated power supply is correctly installed and seated in the director. If required, partially remove and reseal the power supply.

Was a corrective action performed?

**YES**      **NO**

↓              Go to [step 7](#).

---

## 6

Verify redundant power supply operation.

1. Inspect the power supply and ensure the green **PWR OK** LED illuminates and all amber LEDs extinguish.
2. At the Hardware View, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

**YES**      **NO**

↓              The director is operational. **Exit MAP.**

---

## 7

A redundant power supply failed and must be removed and replaced (“[RRP: Redundant Power Supply](#)” on page 245).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**Note:** Do not remove a power supply unless a replacement is immediately available. To avoid director overheating, a power supply must be replaced within five minutes.

---

Did power supply replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 8

Power sense circuitry is defective in the indicated power supply or there is a problem with facility input power.

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 100 and 240 VAC, and between 2 and 4 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

**NO**            **YES**

↓            Go to [step 7](#).

Ask the customer to correct the facility power problem. When facility power is corrected. **Continue.**

---

## 9

Verify director operation:

1. Inspect the director front bezel and ensure the green power LED illuminates. Inspect the active CTP2 card and ensure the green LED illuminates.
2. Inspect both power supplies. Ensure both green **PWR OK** LEDs illuminate and all amber LEDs extinguish.
3. At the Hardware View, observe all graphics representing FRUs and power supplies, and ensure emulated green LEDs illuminate.

Is a failure indicated?

**YES**            **NO**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

---

## 10

Is fault isolation being performed at the director?

**YES**      **NO**

↓      Fault isolation is being performed at the HAFM appliance or Embedded Web Server interface. Go to [step 21](#).

---

## 11

Verify the director is connected to facility power and is powered on.

1. Ensure AC power cords (**PS0** and **PS1**) are connected to the rear of the director and to facility power receptacles. If not, connect the cords as directed by the customer.
2. Ensure associated facility circuit breakers are on. If not, ask the customer to set the circuit breakers on.
3. Ensure the AC power cords are not damaged. If damaged, replace the cords.
4. Ensure the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position.

**Continue.**

---

## 12

Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**      **NO**

↓      Go to [step 14](#).

---

## 13

Does inspection of a power supply indicate a failure (green **PWR OK** LED extinguished and one or more amber LEDs illuminated)?

**NO**            **YES**

↓                    A redundant power supply failed. Go to [step 7](#).

The director is operational. **Exit MAP.**

---

## 14

The director's AC power distribution system failed. Possible causes include failure of:

- Both power supplies.
- Power module assembly.
- Backplane.

Does inspection of both power supplies indicate a dual failure (both green **PWR OK** LEDs extinguished and one or more amber LEDs illuminated on each power supply)?

**YES**            **NO**

↓                    One or both power supplies are operational, but a power distribution failure through the backplane is indicated. Go to [step 19](#).

---

## 15

Ensure both power supplies are correctly installed and seated in the director. If required, partially remove and reseal the power supplies.

Was a corrective action performed?

**YES**            **NO**

↓                    Go to [step 17](#).

---

## 16

Verify operation of both power supplies.

1. Inspect the power supplies and ensure the green **PWR OK** LEDs illuminate and all amber LEDs extinguish.
2. At the Hardware View, observe the graphics representing the power supplies and ensure failure symbols (blinking red and yellow diamonds) do not display.

Is a dual power supply failure still indicated?

**YES**            **NO**

↓            The director is operational. **Exit MAP.**

---

## 17

Both power supplies failed and must be removed and replaced (“[RRP: Redundant Power Supply](#)” on page 245). Perform the data collection procedure as part of FRU removal and replacement.

Did dual power supply replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

A dual power supply failure is not confirmed. Replace both original power supplies to avoid the cost of expending replacement FRUs. **Continue.**

---

## 18

A power module assembly failure is indicated and must be removed and replaced (“[RRP: Power Module Assembly](#)” on page 255). This procedure is non-concurrent and must be performed while director power is off.

Did power module assembly replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

A power module assembly failure is not confirmed. Replace the original power module assembly to avoid the cost of expending a replacement FRU. **Continue.**

---

## 19

One or both power supplies are operational, but logic cards are not receiving DC power. In-card circuit breakers for all logic cards may have tripped due to a power surge, or the backplane failed.

Power cycle the director to reset all logic cards (“[Power-On Procedure](#)” on page 200).

Did power cycling the director solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

---

## 20

The backplane failed and must be removed and replaced (“[RRP: Backplane](#)” on page 258).

- This procedure is non-concurrent and must be performed while director power is off.
- Perform the data collection procedure as part of FRU removal and replacement.

Did backplane replacement solve the problem?

**NO**                      **YES**

↓                      The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 21

Is fault isolation being performed at the HAFM appliance?

**YES**                      **NO**

↓                      Fault isolation is being performed at the Embedded Web Server interface. Go to [step 25](#).

---

## 22

At the Hardware View, does a yellow triangle display at the alert panel and a blinking red and yellow diamond (failed FRU indicator) display over a power supply graphic?

**NO**                      **YES**

↓                      A redundant power supply failed. Go to [step 7](#).

---

## 23

At the Hardware View, does a grey square display at the alert panel, a No Link status displays at the director Status table, and graphical FRUs are uninstalled?

**YES**                      **NO**

↓                      A green circle displays at the alert panel and the director is operational. **Exit MAP.**

The grey square indicates the HAFM appliance cannot communicate with the director because:

- The director-to-HAFM appliance Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**

---

## 24

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**



Go to [step 14](#).

Analysis for an Ethernet link or dual CTP2 card failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**

---

## 25

Is the Embedded Web Server interface operational?

**NO**            **YES**



Go to [step 28](#).

---

## 26

A Page cannot be found, Unable to locate the server, HTTP 404-file not found, or other similar message displays. The message indicates the Web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**

---

## 27

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**



Go to [step 14](#).

Analysis for an Ethernet link or dual CTP2 card failure is not described in this MAP. Go to "[MAP 0000: Start MAP](#)" on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**



---

## 28

Inspect power supply operational states at the Embedded Web Server interface.

1. At the View panel, click the **FRU Properties** tab. The View panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a **Failed** message for either power supply?

**NO**                      **YES**

↓                      A redundant power supply failed. Go to [step 7](#).

The director is operational. **Exit MAP.**

## MAP 0200: POST Failure Analysis

When the director is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the director performs an initial program load (IPL) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IPL process.

If an error is detected, the POST/IPL process continues in an attempt to initialize the director and bring it online. An event code **400** is displayed when the director completes the POST/IPL process.

---

### 1

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**                      **NO**

↓                      An AC power distribution problem is indicated, and analysis for the failure is not described in this MAP. Go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

## 2

Was an event code **400**, or **411**, or **413** observed at the director Event Log (HAFM appliance) or at the Embedded Web Server Event Log?

**YES**      **NO**



Analysis for the failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. **Exit MAP.**

## 3

[Table 7](#) lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

**Table 7: MAP 0200: Event Codes**

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to <a href="#">step 4</a>
411	Firmware fault.	Go to <a href="#">step 11</a>
413	Backup CTP2 card POST failure.	Go to <a href="#">step 12</a>

## 4

POST/IPL diagnostics detected an FRU failure as indicated by an event code **400** with supplementary event data.

1. At the Hardware View, click **Logs > Event Log**. The Event Log displays.
2. Examine the first two bytes (**0** and **1**) of event data.

Byte **0** is an FRU code that indicates the failed component. Byte **1** is the slot number of the failed FRU (**00** for a nonredundant FRU, **00** or **01** for redundant FRUs, and **00** through **15** for UPM cards).

[Table 8](#) lists byte **0** FRU codes and associated steps that describe fault isolation procedures.

**Table 8: Byte 0 FRU Codes**

Byte 0	Failed FRU	Action
01	Backplane.	Go to <a href="#">step 5</a>
02	CTP2 card.	Go to <a href="#">step 6</a>
03	SBAR assembly.	Go to <a href="#">step 7</a>

**Table 8: Byte 0 FRU Codes**

Byte 0	Failed FRU	Action
05	Fan module.	Go to <a href="#">step 8</a>
06	Power supply.	Go to <a href="#">step 9</a>
08-0F	UPM card.	Go to <a href="#">step 10</a>

---

## 5

The backplane failed POSTs (indicated by a **01** FRU code) and must be removed and replaced (“[RRP: Backplane](#)” on page 258).

- This procedure is non-concurrent and must be performed while director power is off.
- Perform the data collection procedure as part of FRU removal and replacement.

Did backplane replacement solve the problem?

**NO**                      **YES**

↓                      The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 6

A CTP2 card failed POSTs (indicated by a **02** FRU code) and must be removed and replaced (“[RRP: Redundant CTP2 Card](#)” on page 231).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**Note:** Do not remove and replace a redundant CTP2 card if the backup CTP2 card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

---

Did CTP2 card replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 7

An SBAR assembly failed POSTs (indicated by a **03** FRU code) and must be removed and replaced (“[RRP: Redundant SBAR Assembly](#)” on page 248).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did SBAR assembly replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 8

A fan module failed POSTs (indicated by a **05** FRU code) and must be removed and replaced (“[RRP: Redundant Fan Module](#)” on page 252).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**Note:** Do not remove a fan module unless the replacement module is available. Operation of the director with only one fan module for an extended period may cause one or more thermal sensors to post event codes.

---

Did fan module replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 9

A power supply failed POSTs (indicated by a **06** FRU code) and must be removed and replaced (“**RRP: Redundant Power Supply**” on page 245).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**Note:** Do not remove a power supply unless a replacement is immediately available. To avoid director overheating, a power supply must be replaced within five minutes.

---

Did power supply replacement solve the problem?

**NO**                      **YES**

↓

The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 10

A UPM card failed POSTs (indicated by a **08** through **0F** FRU code) and must be removed and replaced (“**RRP: UPM Card**” on page 236).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did UPM card replacement solve the problem?

**NO**                      **YES**

↓

The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 11

POST/IPL diagnostics detected a firmware failure (as indicated by an event code **411**) and performed an online dump. All Fibre Channel ports reset after the failure and devices momentarily log out, log in, and resume operation.

Perform the data collection procedure and return the information to HP for analysis by third-level support personnel. **Exit MAP.**

---

## 12

The backup CTP2 card failed POST/IPL diagnostics (as indicated by an event code **413**) and must be removed and replaced (“[RRP: Redundant CTP2 Card](#)” on page 231).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**Note:** Do not remove and replace a redundant CTP2 card if the backup CTP2 card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

---

Did CTP2 card replacement solve the problem?

**NO**                      **YES**

↓                      The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## MAP 0300: HAFM Appliance Software Problem Determination

This map describes isolation of HAFM appliance problems, including problems associated with the Windows 2000 operating system, *HAFM* application, and Element Manager.

### 1

Did the HAFM appliance lock up or crash without displaying a warning or error message?

**YES**

**NO**



Go to [step 4](#).

### 2

An application or operating system problem is indicated. Close the *HAFM* application (at the browser-capable PC connected through an Ethernet LAN segment to the HAFM appliance).

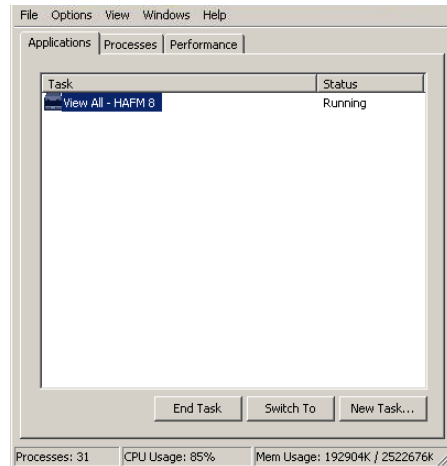
1. At the HAFM appliance Windows 2000 desktop, click the **Send Ctrl-Alt-Del** button at the top of the window. The Windows Security dialog box displays, as shown in [Figure 18](#).

**Note:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action controls the browser-capable PC, not the HAFM appliance.



**Figure 18: Windows Security dialog box**

2. At the Windows 2000 Security dialog box, click **Task Manager**. The Windows 2000 Task Manager dialog box displays with the **Applications** tab open, as shown in [Figure 19](#).



**Figure 19: Task Manager dialog box, Applications tab**

3. Click the *View All - HAFM 8* entry and then click **End Task**. The *HAFM* application closes.
4. Close the Task Manager dialog box.

**Continue.**

---

### 3

Attempt to clear the problem by rebooting the HAFM appliance.

1. Click **Start > Shut Down**. The Shut Down Windows dialog box displays.
2. Click **Shut down** on the drop-down list and then click **OK** to power off the HAFM appliance.
3. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the HAFM appliance and perform power-on self-tests (POSTs). During POSTs:
  - a. The green LCD panel illuminates.
  - b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.



- c. After a few seconds, the LCD panel displays a message, as shown in [Figure 8](#) on page 48.
- d. Ignore the message. After ten seconds, the HAFM appliance performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the appliance performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name
  - System date and time
  - LAN 1 and LAN 2 IP addresses
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed
  - Central processing unit (CPU) temperature
  - Hard disk capacity
  - Virtual and physical memory capacity
4. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
5. After rebooting the server at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. The *HAFM* application starts and the HAFM 8 Log In dialog box displays, as shown in [Figure 9](#) on page 49.
6. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*. The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.

If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.
7. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
8. If you want your computer to save the login information, click the **Save Password** option.
9. Click **Login**. The View All - HAFM 8 window displays, as shown in [Figure 10](#) on page 50.

Did the View All - HAFM 8 window display and is the *HAFM* application operational?

**NO**            **YES**

↓            The problem is transient and the HAFM appliance is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 4

Did the *HAFM* application display a dialog box with the message Connection to HAFM appliance lost-click OK to exit application or HAFM application error *n* (where *n* is an error message number **1** through **8** inclusive)?

**NO**            **YES**

↓            A *HAFM* application error occurred. Click **OK** to close the dialog box and close the application. Go to [step 3](#).

---

## 5

Did the *HAFM* application display a dialog box with the message The software version on this HAFM appliance is not compatible with the version on the remote HAFM appliance?

**YES**            **NO**

↓            Go to [step 8](#).

---

## 6

The *HAFM* applications running on the HAFM appliance and client workstation are not at compatible release levels. Recommend to the customer that the downlevel version be upgraded.

Does the customer want the *HAFM* application upgraded?

**YES**            **NO**

↓            Power off the client workstation. **Exit MAP.**

---

**7**

Upgrade the downlevel *HAFM* application (“[Install or Upgrade Software](#)” on page 223).

Did the software upgrade solve the problem?

**NO**            **YES**

↓            The HAFM appliance is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

**8**

Did the Element Manager display a dialog box with the message Element Manager error 5001 or Element Manager error 5002?

**NO**            **YES**

↓            An Element Manager error occurred. Click **OK** to close the dialog box, and close the *HAFM* application and the Element Manager. Go to [step 3](#).

---

**9**

Did the Element Manager display a dialog box with the message Send firmware failed?

**YES**            **NO**

↓            Go to [step 11](#).

---

**10**

An attempt to download a firmware version from the HAFM appliance hard drive to the director failed. Retry the operation (“[Manage Firmware Versions](#)” on page 211).

Did the firmware version download to the director?

**NO**            **YES**

↓            The HAFM appliance is operational. **Exit MAP.**

A CTP2 card failure is suspected. Go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem. **Exit MAP.**

---

## 11

Did the Element Manager display a dialog box with the message The data collection process failed?

**YES**            **NO**

↓            Go to [step 13](#).

---

## 12

The data collection process failed. Retry the process using a new backup CD ("[Collecting Maintenance Data](#)" on page 197).

Did the data collection process complete?

**NO**            **YES**

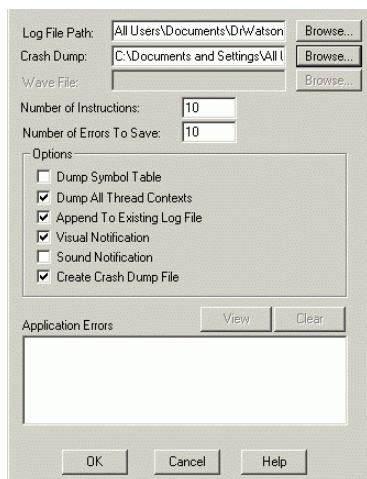
↓            Return the backup CD to HP for analysis by third-level support. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 13

Did the HAFM appliance lock up or crash and display a Dr. Watson for Windows 2000 dialog box, as shown in [Figure 20](#)?



**Figure 20: Dr. Watson for Windows dialog box**

**YES**      **NO**

↓      Go to [step 14](#).

A Windows 2000 operating system or *HAFM* application error occurred and transmitted a handling exception event to the operating system.

1. Click **Cancel** to close the Dr. Watson for Windows 2000 dialog box and *HAFM* application.
2. Using the **My Computer** function at the Windows 2000 desktop, copy the crash dump file (*user.dmp*) from the local disk (C :) to the CD-RW drive (D :).
3. At the HAFM appliance, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
4. Remove the CD and return it to HP customer support personnel for analysis.

Go to [step 3](#).

---

## 14

Did the HAFM appliance crash and display a blue screen with the system dump file in hexadecimal format (“blue screen of death”)?

**YES**      **NO**

↓      The HAFM appliance is operational. **Exit MAP.**

---

## 15

Attempt to clear the problem by power cycling the HAFM appliance.

1. At the rack-mount HAFM appliance, press the power (⏻) button on the LCD panel to power off the appliance.
2. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the server and perform power-on self-tests (POSTs). During POSTs:
  - a. The green LCD panel illuminates.
  - b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  - c. After a few seconds, the LCD panel displays a message, as shown in [Figure 8](#) on page 48.

- d. Ignore the message. After ten seconds, the appliance performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - Central processing unit (CPU) temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
3. After successful POST completion, the LCD panel displays a *Welcome!!* message, then continuously cycles through and displays appliance operational information.
4. After rebooting the server at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. The *HAFM* application starts and the HAFM 8 Log In dialog box displays, as shown in [Figure 9](#) on page 49.
5. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*. The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.

If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.
6. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
7. If you want your computer to save the login information, click **Save Password**.
8. Click **Login**. The View All - HAFM 8 window displays, as shown in [Figure 10](#) on page 50.

Did the View All - HAFM 8 window display and is the *HAFM* application operational?

**NO**                      **YES**



The problem is transient and the HAFM appliance is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## MAP 0400: Loss of HAFM or Web Browser PC Communication

This MAP describes fault isolation of the Ethernet communication link between a director and the HAFM appliance, or between a director and a Web browser PC running the Embedded Web Server interface. Failure indicators include:

- At the HAFM main window, a grey square with an exclamation mark associated with the icon representing the director reporting the problem.
- At the Hardware View, a grey square at the alert panel, a No Link status and reason at the director Status table, and no FRUs visible for the director.
- At the Web browser PC, a Page cannot be found, Unable to locate the server, HTTP 404-file not found, or other similar message.
- Event codes recorded at the director Event Log or Embedded Web Server Event Log.

When the logical connection between the director and HAFM appliance is initiated, it may take up to five minutes for the link to activate. This delay is normal.



**Caution:** Prior to servicing a director or HAFM appliance, determine the Ethernet LAN configuration. Installation of directors and the HAFM appliance on a public customer intranet can complicate problem determination and fault isolation.

### 1

Was an event code **430**, **431**, or **432** observed at the director Event Log (HAFM appliance) or at the Embedded Web Server Event Log?

**YES**                      **NO**



Go to [step 3](#).

## 2

Table 9 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 9: MAP 0400: Event Codes**

Event Code	Explanation	Action
430	Excessive Ethernet transmit errors.	Go to <a href="#">step 8</a>
431	Excessive Ethernet receive errors.	Go to <a href="#">step 8</a>
432	Ethernet adapter reset.	Go to <a href="#">step 14</a>

---

## 3

Is fault isolation being performed at the HAFM appliance?

**YES**      **NO**



Fault isolation is being performed through the Embedded Web Server interface. Go to [step 24](#).

---

## 4

At the HAFM main window, is a grey square with yellow exclamation mark associated with the icon representing the director reporting the problem?

**YES**      **NO**



The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

The grey square indicates the HAFM appliance cannot communicate with the director because:

- The director-to-HAFM appliance Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**



---

## 5

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**      **NO**

↓      A power distribution problem is indicated. Go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 6

At the director, inspect the amber LED at the top of each CTP2 card.

Is the amber LED illuminated on both CTP2 cards?

**NO**      **YES**

↓      Failure of both CTP2 cards is indicated. Go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

## 7

The director-to-HAFM appliance Ethernet link failed. Perform the following:

1. At the physical map, right-click the icon with the grey square and exclamation mark representing the director or switch reporting the problem. A pop-up menu displays.
2. Click **Element Manager**. The Hardware View displays and the following occurs:
  - A grey square displays at the alert panel.
  - No FRUs are visible for the director.
  - The Director 2/64 Status table is yellow, the **Status** field displays **No Link**, and a reason for the link failure.

[Table 10](#) lists the link failure reasons and associated steps that describe fault isolation procedures.

**Table 10: MAP 0400: Error Messages and Actions**

Error Message	Action
Never connected.	Go to <a href="#">step 8</a>
Link timeout.	Go to <a href="#">step 8</a>
Protocol mismatch.	Go to <a href="#">step 15</a>
Duplicate session.	Go to <a href="#">step 18</a>
Unknown network address.	Go to <a href="#">step 21</a>
Incorrect product type.	Go to <a href="#">step 23</a>

---

## 8

Transmit or receive errors for a director's Ethernet adapter (on each CTP2 card) exceeded a threshold, the director-to-HAFM appliance link was not connected, or the director-to-HAFM appliance link timed out. A problem with the Ethernet cable, Ethernet hub or hubs, or other LAN-attached device is indicated.

Verify the director is connected to the HAFM appliance through one or more Ethernet hubs.

1. Ensure an RJ-45 Ethernet cable connects both of the director's CTP2 cards to an Ethernet hub. If not, connect the cables as directed by the customer.
2. Ensure an RJ-45 Ethernet cable connects the HAFM appliance adapter card to an Ethernet hub. If not, connect the cable as directed by the customer.
3. Ensure the Ethernet cables are not damaged. If damaged, replace the cables.

Was a corrective action performed?

**NO**                      **YES**

↓                      Go to [step 1](#).

---

## 9

Does the LAN configuration use multiple (up to four) Ethernet hubs that are daisy-chained?

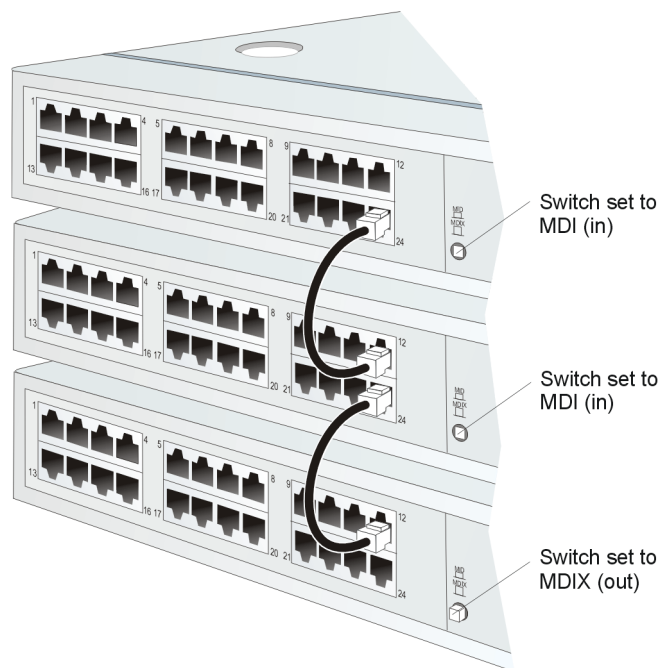
**YES**                      **NO**

↓                      Go to [step 11](#).

---

## 10

If appropriate, verify that the hubs are correctly daisy-chained, as shown in [Figure 21](#).



**Figure 21: Ethernet Hubs, Daisy-Chained**

---

**Note:** To check two hubs, use [step 1](#) and [step 2](#) (top and middle hub instructions only).

---

1. At the first (top) Ethernet hub, ensure an RJ-45 Ethernet patch cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDI (in)**.
2. At the middle Ethernet hub, ensure the patch cable from the top hub connects to port **12**, the patch cable from the bottom hub connects to port **24**, and the MDI switch is set to **MDI (in)**.
3. At the bottom Ethernet hub, ensure the patch cable from the middle hub connects to port **12** and the MDI switch is set to **MDIX (out)**.

Was a corrective action performed?

**NO**            **YES**

↓            Go to [step 1](#).

---

## 11

Verify operation of the Ethernet hub or hubs. Inspect each hub for indications of being powered on, such as:

- Green Power LED illuminated.
- Green Status LEDs illuminated.

Is a hub failure indicated?

**YES**            **NO**

↓            Go to [step 13](#).

---

## 12

Remove and replace the Ethernet hub. Refer to the supporting documentation shipped with the hub for instructions.

Did hub replacement solve the problem?

**NO**            **YES**

↓            The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 13

A problem with another LAN-attached device is indicated.

- If the problem is associated with another director or HAFM appliance, go to 2 to isolate the problem for that device. **Exit MAP.**
- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

**NO**            **YES**

↓            The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

---

**14**

The Ethernet adapter on the director's active CTP2 card reset in response to an error. The connection to the HAFM appliance terminated briefly, then recovered upon reset.

Perform the data collection procedure and return the backup CD to HP for analysis by third-level support personnel. **Exit MAP.**

---

**15**

A protocol mismatch occurred because the *HAFM* application (running on the HAFM appliance) and the director firmware are not at compatible release levels. Recommend to the customer that the downlevel version (software or firmware) be upgraded.

Does the *HAFM* application require upgrade?

**YES**            **NO**

↓

Go to [step 17](#).

---

**16**

Upgrade the *HAFM* application (“[Install or Upgrade Software](#)” on page 223).

Did the director-to-HAFM appliance Ethernet connection recover?

**NO**            **YES**

↓

The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

**17**

A director firmware upgrade is required (“[Download a Firmware Version to a Director](#)” on page 215). Perform the data collection procedure after the download.

Did the director-to-HAFM appliance Ethernet connection recover?

**NO**            **YES**

↓

The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 18

An instance of the *HAFM* application is open at another HAFM appliance and communicating with the director (duplicate session). Notify the customer and either:

- Power off the HAFM appliance running the second instance of the application, or
- Configure the HAFM appliance running the second instance of the application as a client workstation.

Does the customer want the second HAFM appliance configured as a client?

**YES**

**NO**



Power off the HAFM appliance reporting the **Duplicate Session** communication problem. **Exit MAP.**

---

## 19

Determine the internet protocol (IP) address of the HAFM appliance running the first instance of the *HAFM* application.

1. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays the following operational information:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - CPU temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
2. After a few seconds, the LCD panel displays the following, as shown in [Figure 22](#).



LAN 2:  
010.001.001.001

**Figure 22: LCD panel (LAN 2 IP address)**

- Depending on switch-to-server LAN connectivity, record the appropriate IP address (LAN 1 or LAN 2).

**Continue.**

## 20

Configure the HAFM appliance reporting the **Duplicate Session** communication problem as a client.

- At the HAFM main window, click **SAN > Logout**. The HAFM 8 Log In dialog box displays.
- Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*.  
The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.  
If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.
- Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
- If you want your computer to save the login information, click **Save Password**.
- Click **Login**. The View All - HAFM 8 window displays, as shown in [Figure 10](#) on page 50.

Did the HAFM appliance reconfigure as a client and did the Ethernet connection recover?

**NO**

**YES**



The director-to-HAFM appliance connection is restored, and the second HAFM appliance is operational as a client. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 21

The IP address defining the director to the *HAFM* application is incorrect or unknown and must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the director's IP address. The tools are provided with the director or by service personnel. To verify the IP address:

1. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a Phillips-tip screwdriver may be required). Connect one end of the RS-232 null modem cable to the port.
2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.
4. Click **Start > Programs > Accessories > Communications > HyperTerminal**. The Connection Description dialog box displays.

---

**Note:** The following steps describe inspecting the IP address using HyperTerminal serial communication software.

---

5. Type 64 in the **Name** field and click **OK**. The Connect To dialog box displays.
6. Ensure the **Connect using** field displays **COM1** or **COM2** (depending on the serial communication port connection to the director), and click **OK**. The COMn Properties dialog box displays (where n is 1 or 2).
7. Configure the **Port Settings** parameters as follows:
  - Bits per second-**57600**.
  - Data bits-**8**.
  - Parity-**None**.
  - Stop bits-**1**.
  - Flow control-**Hardware**.

When the parameters are set, click **OK**. The Director 2/64 HyperTerminal window displays.



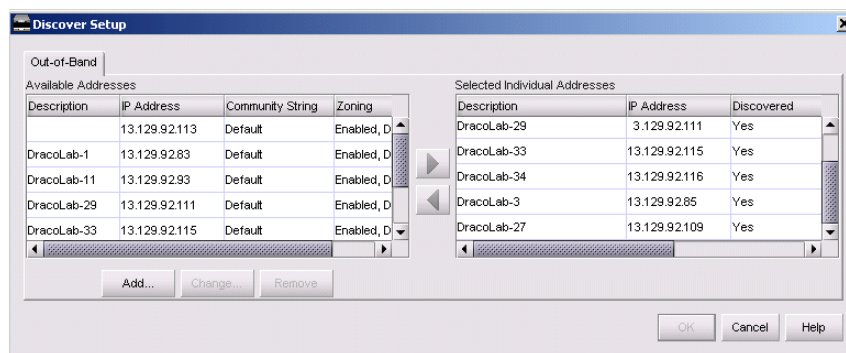
8. At the > prompt, type the user-level password (the default is **password**) and press the **Enter** key. The password is case-sensitive. The Director 2/64 HyperTerminal window displays with a **C>** prompt at the bottom of the window.
9. At the **C>** prompt, type the **ipconfig** command and press the **Enter** key. The Director 2/64 HyperTerminal window displays with configuration information listed (including the IP address).
10. Record the director's IP address.
11. Click **File > Exit**. A HyperTerminal dialog box displays.
12. Click **Yes**. A second HyperTerminal dialog box displays.
13. Click **No** to exit and close the *HyperTerminal* application.
14. Power off the maintenance terminal.
15. Disconnect the RS-232 null modem cable from the director and the maintenance terminal. Replace the protective cap over the maintenance port.

**Continue.**

## 22

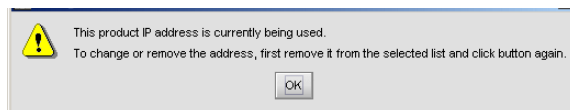
Define the director's correct IP address to the HAFM appliance.

1. At the HAFM main window, click **Discover > Setup**. The Discover Setup dialog box displays, as shown in [Figure 23](#).



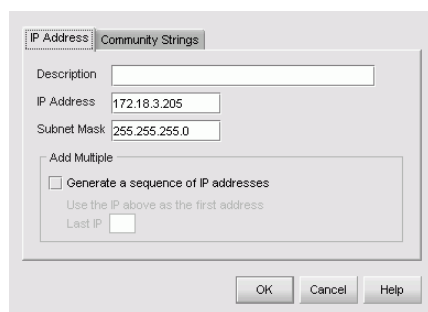
**Figure 23: Discover Setup dialog box**

- Highlight the director to be reconfigured from the **Available Addresses** list, and click **Change**. The Editing Domain Information dialog box displays, as shown in [Figure 24](#).



**Figure 24: Editing Domain Information dialog box**

- Click **OK**. The Domain Information dialog box displays with the IP Address page open, as shown in [Figure 25](#).



**Figure 25: Domain Information dialog box (IP Address page)**

- Enter the correct IP address in the **IP Address** field.
- Click **OK** to save the new IP address, close the dialog box, and redefine the director to the *HAFM* application.
- Click **OK** to close the Discover Setup dialog box.

At the HAFM master log, did the IP address below the director icon change to the new entry and did the Ethernet connection recover?

**NO**                      **YES**



The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 23

An incorrect product type is defined to the HAFM appliance.

1. At the HAFM main window, right-click the icon with the grey square and yellow exclamation point (representing the product reporting the problem) at the Physical Map. A menu displays.
2. Click **Delete**. A Warning dialog box displays, as shown in [Figure 26](#).



**Figure 26: HAFM message dialog box**

3. Click **Yes** to delete the director.
4. At the HAFM main window, click **Discover > Setup**. The Discover Setup dialog box displays, as shown in [Figure 23](#) on page 105.
5. Click **Add**. The Domain Information dialog box displays with the IP Address page open, as shown in [Figure 25](#) on page 106.
6. Enter a description for the product in the **Description** field.
7. Enter the IP address in the **IP Address** field.
8. Enter the subnet mask associated with the IP address in the **Subnet Mask** field.
9. Click **OK**.
10. Click **OK** to close the Discover Setup dialog box.

At the HAFM master log, did the IP address below the director icon change to the new entry and did the Ethernet connection recover?

**NO**                      **YES**

↓                      The director-to-HAFM appliance connection is restored and is operational. **Exit MAP.**

## 24

Is the Embedded Web Server interface operational?

**NO**                      **YES**

↓                      The director-to-web server PC connection is restored and is operational. **Exit MAP.**

---

## 25

A Page cannot be found, Unable to locate the server, HTTP 404-file not found, or other similar message displays. The message indicates the Web browser PC cannot communicate with the director because:

- The director-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**

---

## 26

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**



A power distribution problem is indicated. Go to “[MAP 0100: Power Distribution Analysis](#)” on page 71. **Exit MAP.**

---

## 27

At the director, inspect the amber LED at the top of each CTP2 card.

Is the amber LED illuminated on both CTP2 cards?

**NO**            **YES**



Failure of both CTP2 cards is indicated. Go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

---

## 28

Either a director-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a director Ethernet port failure is indicated.

1. Wait approximately five minutes, then attempt to log in to the director again.
2. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the director (obtained in “[MAP 0000: Start MAP](#)” on page 46). The Username And Password Required dialog box displays.
3. Type the user name and password obtained in “[MAP 0000: Start MAP](#)” on page 46 and click **OK**. If the View panel does not display, wait five minutes and perform this step again.

Is the Embedded Web Server interface operational with the View panel displayed?

<b>NO</b>	<b>YES</b>
-----------	------------

↓

The director-to-Web server PC connection is restored and is operational. **Exit MAP.**

Failure of the CTP2 card's Ethernet port is indicated. Go to “[MAP 0500: FRU Failure Analysis](#)” on page 110. **Exit MAP.**

## MAP 0500: FRU Failure Analysis

This MAP describes fault isolation for the CTP2 card, SBAR assembly, and fan module. Failure indicators include:

- The amber LED on the FRU illuminates.
- The amber emulated LED on a fan graphic at the Hardware View illuminates.
- A blinking red and yellow diamond (failed FRU indicator) displays over an FRU graphic, or a grey square (status unknown indicator) or yellow triangle (attention indicator) displays at the alert panel of the HAFM main window or Hardware View.
- An event code recorded at the director Event Log or the Embedded Web Server Event Log.
- A Failed message associated with an FRU at the Embedded Web Server interface.

### 1

Was an event code **300, 301, 302, 303, 304, 305, 414, 420, 426, 433, 440, 604, 605, 607, 805, 806, 807, 810, 811, 812, or 850** observed at the director Event Log (HAFM appliance) or at the Embedded Web Server Event Log?

**YES**

**NO**



Go to [step 3](#).

### 2

[Table 11](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 11: MAP 0500: Event Codes**

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to <a href="#">step 5</a>
301	Cooling fan propeller failed.	Go to <a href="#">step 5</a>
302	Cooling fan propeller failed.	Go to <a href="#">step 5</a>
303	Cooling fan propeller failed.	Go to <a href="#">step 5</a>
304	Cooling fan propeller failed.	Go to <a href="#">step 5</a>
305	Cooling fan propeller failed.	Go to <a href="#">step 5</a>
414	Backup CTP2 card failed.	Go to <a href="#">step 7</a>

**Table 11: MAP 0500: Event Codes (Continued)**

Event Code	Explanation	Action
420	Backup CTP2 card NV-RAM failure.	Go to <a href="#">step 7</a>
426	Multiple ECC single-bit errors occurred.	Go to <a href="#">step 7</a>
433	Non-recoverable Ethernet fault.	Go to <a href="#">step 7</a>
440	Embedded port hardware failed.	Go to <a href="#">step 7</a>
604	SBAR assembly failure.	Go to <a href="#">step 9</a>
605	SBAR assembly revision not supported.	Go to <a href="#">step 16</a>
607	Director contains no operational SBAR assemblies.	Go to <a href="#">step 9</a>
805	High temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">step 9</a>
806	Critically hot temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">step 9</a>
807	SBAR assembly shutdown due to thermal violation.	Go to <a href="#">step 9</a>
810	High temperature warning (CTP2 card thermal sensor).	Go to <a href="#">step 7</a>
811	Critically hot temperature warning (CTP2 card thermal sensor).	Go to <a href="#">step 7</a>
812	CTP2 card shutdown due to thermal violation.	Go to <a href="#">step 7</a>
850	System shutdown due to CTP2 card thermal violations.	Go to <a href="#">step 7</a>

**3**

Is fault isolation being performed at the director?

**YES****NO**

Fault isolation is being performed at the HAFM appliance or Embedded Web Server interface. Go to [step 10](#).

---

## 4

Inspect both fan modules at the rear of the director. Fan module LEDs can be inspected through the hexagonal cooling vents of the radio frequency interference (RFI) shield.

Does inspection of a director fan module indicate a failure? Indicators include:

- The amber LED is illuminated but not blinking (beaconing) on one or both fan modules.
- One or more cooling fans are not rotating.

**YES**

**NO**

↓

Go to [step 6](#).

---

## 5

One or more cooling fans failed, and one or both fan modules must be removed and replaced (“[RRP: Redundant Fan Module](#)” on page 252).

- If one or more fans in a module are operating, do not remove the fan module unless the replacement is immediately available.
- If a multiple fan failure caused a thermal shutdown, power on the director after the fan modules are replaced (“[Power-On Procedure](#)” on page 200).

---

**Note:** Do not remove a fan module unless the replacement module is available. Operation of the director with only one fan module for an extended period may cause one or more thermal sensors to post event codes.

---

Are the fan modules functioning?

**NO**

**YES**

↓

The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**



---

## 6

Inspect the faceplates of both CTP2 cards at the front of the director.

Is the amber LED at the top of a CTP2 card illuminated but not blinking (beaconing)?

**YES**            **NO**

↓                    Go to [step 8](#).

---

## 7

A CTP2 card failed and must be removed and replaced (“[RRP: Redundant CTP2 Card](#)” on page 231).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**Note:** Do not remove and replace a CTP2 card if the backup CTP2 card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

---

Did CTP2 card replacement solve the problem?

**NO**            **YES**

↓                    The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 8

Inspect both SBAR assemblies at the rear of the director. SBAR assembly LEDs can be inspected through the hexagonal cooling vents of the RFI shield.

Is the amber LED on an SBAR assembly illuminated but not blinking (beaconing)?

**YES**            **NO**

↓                    The director is operational. **Exit MAP.**

---

## 9

An SBAR assembly failed and must be removed and replaced (“[RRP: Redundant SBAR Assembly](#)” on page 248).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did SBAR assembly replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 10

Is fault isolation being performed at the HAFM appliance?

**YES**            **NO**

↓            Fault isolation is being performed at the Embedded Web Server interface. Go to [step 18](#).

---

## 11

Is a blinking red and yellow diamond (failed FRU indicator) overlaying a fan module graphic at the Hardware View?

**NO**            **YES**

↓            A fan module failure is indicated. Go to [step 5](#).

---

## 12

Is a blinking red and yellow diamond (failed FRU indicator) overlaying a CTP2 card graphic at the Hardware View?

**NO**            **YES**

↓            A CTP2 card failure is indicated. Go to [step 7](#).

---

## 13

Is a blinking red and yellow diamond (failed FRU indicator) overlaying an SBAR assembly graphic at the Hardware View?

**NO**            **YES**

↓            An SBAR assembly failure is indicated. Go to [step 9](#).

---

## 14

At the Hardware View, is a grey square displayed at the alert panel, a No Link status displays at the **Director 2/64 Status** table, and graphical FRUs are uninstalled?

**YES**            **NO**

↓            A green circle displays at the alert panel and the director is operational. **Exit MAP.**

The grey square indicates the HAFM appliance cannot communicate with the director because:

- The director-to-HAFM appliance Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**

---

## 15

At the director, inspect the amber LED at the top of each CTP2 card.

Is the amber LED illuminated on both CTP2 cards?

**NO**            **YES**

↓            Failure of both CTP2 cards is indicated. Go to [step 7](#).

Analysis for an Ethernet link or AC power distribution failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**

---

## 16

An SBAR assembly is not recognized by director firmware because the firmware version is not supported or the SBAR assembly failed. Advise the customer of the problem and determine the correct firmware version to download from the HAFM appliance.

Download the firmware (“[Download a Firmware Version to a Director](#)” on page 215). Perform the data collection procedure after the download. **Continue.**

---

## 17

Did the firmware download solve the problem?

**NO**                **YES**

↓                    The director is operational. **Exit MAP.**

An SBAR assembly failure is indicated. Go to [step 9](#).

---

## 18

Is the Embedded Web Server interface operational?

**NO**                **YES**

↓                    Go to [step 22](#).

---

## 19

A Page cannot be found, Unable to locate the server, HTTP 404-file not found, or other similar message displays. The message indicates the Web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director’s CTP2 cards failed.

**Continue.**

---

## 20

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**            **NO**



Analysis for an AC power distribution failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**

---

## 21

At the director, inspect the amber LED at the top of each CTP2 card.

Is the amber LED illuminated on both CTP2 cards?

**NO**            **YES**



Failure of both CTP2 cards is indicated. Go to [step 7](#).

Analysis for an Ethernet link failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**

---

## 22

Inspect fan module operational states at the Embedded Web Server interface.

1. At the View panel, click the **FRU Properties** tab. The View panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for both fan modules.

Does the **Status** field display a **Failed** message for either fan module?

**NO**            **YES**



A fan module failure is indicated. Go to [step 5](#).

---

**23**

Inspect CTP2 card operational states at the Embedded Web Server interface. Inspect the **Status** fields for both CTP2 cards.

Does the **Status** field display a **Failed** message for either CTP2 card?

**NO**                      **YES**



A CTP2 card failure is indicated. Go to [step 7](#).

---

**24**

Inspect SBAR assembly operational states at the Embedded Web Server interface. Inspect the **Status** fields for both assemblies.

Does the **Status** field display a **Failed** message for either SBAR assembly?

**NO**                      **YES**



An SBAR assembly failure is indicated. Go to [step 9](#).

The director is operational. **Exit MAP.**

## MAP 0600: UPM Card Failure and Link Incident Analysis

This MAP describes fault isolation for Universal Processing Module (UPM) cards, shortwave laser small form factor pluggable (SFP) optical transceivers, and longwave laser SFP optical transceivers; and for Fibre Channel link incidents. Failure indicators include:

- One or more amber LEDs on the UPM card illuminate.
- One or more emulated amber LEDs on a UPM card graphic at the Hardware View illuminate.
- A blinking red and yellow diamond (failed FRU indicator) displays over a UPM card graphic or a yellow triangle (attention indicator) displays at the alert panel of the Hardware View.
- An event code recorded at the Director 2/64 Event Log or the Embedded Web Server Event Log.
- A port operational state message or a **Failed** message associated with a UPM card at the Embedded Web Server interface.
- A link incident message recorded in the Link Incident Log or Port Properties dialog box.

---

**1**

Was an event code **080, 081, 504, 505, 506, 507, 512, 514, 800, 801, or 802** observed at the director Event Log (HAFM appliance) or at the Embedded Web Server Event Log?

**YES**      **NO**

↓      Go to [step 3](#).

---

**2**

Was an event code **581, 582, 583, 584, 585, or 586** observed at the console of an OSI or FICON server attached to the director reporting the problem?

**YES**      **NO**

↓      Go to [step 4](#).

---

**3**

[Table 12](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 12: MAP 0600: Event Codes**

Event Code	Explanation	Action
080	Unauthorized World-Wide Name.	Go to <a href="#">step 18</a>
081	Invalid attachment.	Go to <a href="#">step 20</a>
504	UPM card failure.	Go to <a href="#">step 6</a>
505	UPM card revision not supported.	Go to <a href="#">step 44</a>
506	Fibre Channel port failure.	Go to <a href="#">step 6</a>
507	Loopback diagnostics port failure.	Go to <a href="#">step 14</a>
512	SFP optical transceiver nonfatal error.	Go to <a href="#">step 6</a>
514	SFP optical transceiver failure.	Go to <a href="#">step 6</a>
581	Implicit incident.	Go to <a href="#">step 37</a>
582	Bit error threshold exceeded.	Go to <a href="#">step 37</a>
583	Loss of signal or loss of synchronization.	Go to <a href="#">step 37</a>
584	Not operational primitive sequence received.	Go to <a href="#">step 37</a>
585	Primitive sequence timeout.	Go to <a href="#">step 37</a>

**Table 12: MAP 0600: Event Codes (Continued)**

Event Code	Explanation	Action
586	Invalid primitive sequence received for current link state.	Go to <a href="#">step 7</a>
800	High temperature warning (UPM card thermal sensor).	Go to <a href="#">step 7</a>
801	Critically hot temperature warning (UPM card thermal sensor).	Go to <a href="#">step 7</a>
802	UPM card shutdown due to thermal violation.	Go to <a href="#">step 7</a>

---

**4**

Is fault isolation being performed at the director?

**YES**      **NO**



Fault isolation is being performed at the HAFM appliance or Embedded Web Server interface. Go to [step 8](#).

---

**5**

Inspect the faceplates of UPM cards at the front of the director. Each card has an amber LED (at the top of the card) that illuminates if the card fails or if any Fibre Channel port fails.

Each card also has a bank of amber and green LEDs above the ports. Each LED pair is associated with a corresponding port (for example, the top LED pair is associated with the top port). The amber LED illuminates and the green LED extinguishes if the port fails.

Are an amber port LED and the amber LED at the top of the UPM card illuminated but not blinking (beaconing)?

**YES**      **NO**



The director is operational, however a link incident or other problem may have occurred. Perform fault isolation at the HAFM appliance. Go to [step 8](#).



## 6

A Fibre Channel port failed, and the SFP optical transceiver must be removed and replaced (“RRP: SFP Optical Transceiver” on page 241).

- This procedure is concurrent and can be performed while director power is on.
- Verify location of the failed port. For an OSI environment, [Figure 27](#) and [Figure 28](#) show UPM card numbers (0 through 15) and port numbers (00 through 63). For a FICON environment, [Figure 27](#) and [Figure 28](#) show UPM card numbers (0 through 15), port numbers (00 through 63), and bolded logical port addresses (hexadecimal 04 through 43).

UPM Cards								CTP2 - 1 Card	CTP2 - 0 Card	UPM Cards							
15	14	13	12	11	10	9	8			7	6	5	4	3	2	1	0
63	59	55	51	47	43	39	35			31	27	23	19	15	11	07	03
62	58	54	50	46	42	38	34			30	26	22	18	14	10	06	02
61	57	53	49	45	41	37	33			29	25	21	17	13	09	05	01
60	56	52	48	44	40	36	32			28	24	20	16	12	08	04	00

**Figure 27: UPM card diagram (OSI)**

UPM Cards								CTP2 - 1 Card	CTP2 - 0 Card	UPM Cards							
15	14	13	12	11	10	9	8			7	6	5	4	3	2	1	0
<b>43</b>	<b>3F</b>	<b>3B</b>	<b>37</b>	<b>33</b>	<b>2F</b>	<b>2B</b>	<b>27</b>			<b>23</b>	<b>1F</b>	<b>1B</b>	<b>17</b>	<b>13</b>	<b>0F</b>	<b>0B</b>	<b>07</b>
63	59	55	51	47	43	39	35			31	27	23	19	15	11	07	03
<b>42</b>	<b>3E</b>	<b>3A</b>	<b>36</b>	<b>32</b>	<b>2E</b>	<b>2A</b>	<b>26</b>			<b>22</b>	<b>1E</b>	<b>1A</b>	<b>16</b>	<b>12</b>	<b>0E</b>	<b>0A</b>	<b>06</b>
62	58	54	50	46	42	38	34			30	26	22	18	14	10	06	02
<b>41</b>	<b>3D</b>	<b>39</b>	<b>35</b>	<b>31</b>	<b>2D</b>	<b>29</b>	<b>25</b>			<b>21</b>	<b>1D</b>	<b>19</b>	<b>15</b>	<b>11</b>	<b>0D</b>	<b>09</b>	<b>05</b>
61	57	53	49	45	41	37	33			29	25	21	17	13	09	05	01
<b>40</b>	<b>3C</b>	<b>38</b>	<b>34</b>	<b>30</b>	<b>2C</b>	<b>28</b>	<b>24</b>			<b>20</b>	<b>1C</b>	<b>18</b>	<b>14</b>	<b>10</b>	<b>0C</b>	<b>08</b>	<b>04</b>
60	56	52	48	44	40	36	32			28	24	20	16	12	08	04	00

**Figure 28: UPM card diagram (FICON)**

- Replace the optical transceiver with a transceiver of the same type (shortwave or longwave).
- Perform an external loopback test for the port as part of FRU removal and replacement.

Did optical transceiver replacement solve the problem?

**NO**

**YES**



The director is operational. **Exit MAP.**

## 7

A UPM card failed, and the card must be removed and replaced (“RRP: UPM Card” on page 236).

- This procedure is concurrent and can be performed while director power is on.
- Verify location of the failed card (Figure 27 and Figure 28 on page 121). For an OSI environment, Figure 27 and Figure 28 show UPM card numbers (0 through 15) and port numbers (00 through 63). For a FICON environment, Figure 27 and Figure 28 show UPM card numbers (0 through 15), port numbers (00 through 63), and bolded logical port addresses (hexadecimal 04 through 43).
- Notify the customer that all ports on the defective card are to be blocked. Ensure the customer’s system administrator quiesces Fibre Channel frame traffic through any operational ports on the card and sets attached devices offline.
- Perform an external loopback test for all ports on the replacement card as part of FRU removal and replacement.
- Perform the data collection procedure as part of FRU removal and replacement.

Did UPM card replacement solve the problem?

**NO**                      **YES**



The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 8

Is fault isolation being performed at the HAFM appliance?

**YES**                      **NO**



Fault isolation is being performed at the Embedded Web Server interface. Go to [step 42](#).

---

**9**

Does a blinking red and yellow diamond (failed FRU indicator) display over a UPM card graphic at the Hardware View or display adjacent to a Fibre Channel port graphic at the Port Card View?

**NO**            **YES**



A port or UPM card failure is indicated. Go to [step 6](#).

---

**10**

Did a Fibre Channel port or UPM card (all ports) fail a loopback test?

**NO**            **YES**



Go to [step 14](#).

---

**11**

Does a yellow triangle (attention indicator) display over a UPM card graphic at the Hardware View or display adjacent to a port graphic at the Port Card View?

**YES**            **NO**



Go to [step 13](#).

---

**12**

Inspect the port state and LED status for all ports with an attention indicator.

1. At the Port Card View, double-click the port graphic with the attention indicator. The Port Properties dialog box displays.
2. Inspect the **Operational State** field at the Port Properties dialog box, and the emulated green and amber LEDs adjacent to the port at the Port Card View.
3. [Table 13](#) lists LED and port operational state combinations and associated MAP 0600 (or other) steps that describe fault isolation procedures.

**Table 13: MAP 0600: Port Operational and LED States**

Operational State	Green LED	Amber LED	Action
Offline	Off	Off	Go to <a href="#">step 16</a>
Not Operational	Off	Off	Go to <a href="#">step 16</a>
Testing	Off	Blinking	Internal loopback test in process. <b>Exit MAP.</b>

**Table 13: MAP 0600: Port Operational and LED States (Continued)**

Operational State	Green LED	Amber LED	Action
Testing	On	Blinking	External loopback test in process. <b>Exit MAP.</b>
Beaconing	Off or On	Blinking	Go to <a href="#">step 17</a>
Invalid Attachment	On	Off	Go to <a href="#">step 18</a>
Link Reset	Off	Off	Go to <a href="#">step 32</a>
Link Incident	Off	Off	Go to <a href="#">step 33</a>
Segmented E_Port	On	Off	Go to <a href="#">MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.</a>

## 13

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not display.

At the Hardware View, click **Logs > Link Incident Log**. The Link Incident Log displays. If a link incident occurred, the affected port number is listed with one of the following messages.

Link interface incident-implicit incident.

Link interface incident-bit-error threshold exceeded.

Link failure-loss of signal or loss of synchronization.

Link failure-not-operational primitive sequence (NOS) received.

Link failure-primitive sequence timeout.

Link failure-invalid primitive sequence received for the current link state.

Did one of the listed messages display in the Link Incident Log?

**YES**      **NO**



The director is operational. **Exit MAP.**

Go to [step 33](#).

---

## 14

A Fibre Channel port or UPM card (all ports) failed an internal or external loopback test.

1. Reset each port that failed the loopback test.
  - a. At the Hardware View, right-click the port. A menu displays.
  - b. Click **Reset Port**. A `Reset Port n` message box displays, where n is the port number.
  - c. Click **OK**. The port resets.
2. Perform an external loopback test for all ports that were reset.

Did resetting ports solve the problem?

**NO**                      **YES**



The director is operational. **Exit MAP.**

---

## 15

An electronic circuit breaker on the UPM card may have tripped. To reset the circuit breaker, partially remove and reseat the UPM card for which external loopback tests failed (“[RRP: UPM Card](#)” on page 236).

1. Unseat and disconnect the UPM card from the backplane. Unseat the card only, do not remove it from the director chassis.
2. Reseat the UPM card in the backplane.
3. Perform an external loopback test on the UPM card.

Did reseating the UPM card solve the problem?

**NO**                      **YES**



The director is operational. **Exit MAP.**

Go to [step 7](#).

---

## 16

A director port is unblocked and receiving the offline sequence (OLS) or not operational sequence (NOS) from an attached device.

Inform the customer that the attached device failed or is set offline. **Exit MAP.**

---

## 17

Beaconing is enabled for the port.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.
2. Disable port beaconing.
  - a. At the Hardware View, right-click the port graphic. A menu displays.
  - b. Click **Enable Beaconing**. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

**YES**      **NO**

↓      The director is operational. **Exit MAP.**

Go to [step 1](#).

---

## 18

The eight-byte (16-digit) worldwide name (WWN) entered to configure port binding is not valid or a nickname was used that is not configured for the attached device in the Element Manager.

At the Hardware View, click **Node List**. The Node List dialog box displays. Note the **Port WWN** column. This is the WWN assigned to the port or Fibre Channel interface installed on the attached device.

- If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer name.
- If a nickname is assigned to the WWN, the nickname displays in place of the WWN.

The bound WWN must be entered in the form of a raw WWN format (**XX:XX:XX:XX:XX:XX:XX:XX**) or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Did configuring the WWN or nickname solve the problem?

**NO**      **YES**

↓      The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 19

The port has an invalid attachment. The Reason field in the Port Properties dialog box specifies the reason. See [Table 14](#) for a list of reasons and appropriate actions.

**Table 14: MAP 0600: Invalid Attachment Reasons and Actions**

Reasons	Action
Unknown	Contact the next level of support.
ISL connection not allowed on this port.	Go to <a href="#">step 20</a>
Incompatible switch at other end of ISL.	Go to <a href="#">step 21</a>
External loopback adapter connected to the port.	Go to <a href="#">step 22</a>
N-Port connection not allowed on this port.	Go to <a href="#">step 20</a>
Non-HP switch at other end of the ISL.	Go to <a href="#">step 21</a>
Port binding violation-unauthorized WWN.	Go to <a href="#">step 18</a>
Unresponsive node connected to port.	Go to <a href="#">step 23</a>
ESA security mismatch.	Go to <a href="#">step 28</a>
Fabric binding mismatch.	Go to <a href="#">step 29</a>
Authorization failure reject.	Go to <a href="#">step 23</a>
Unauthorized switch binding WWN.	Go to <a href="#">step 33</a>
Fabric mode mismatch.	Go to <a href="#">step 21</a>
CNT WAN extension mode mismatch.	Go to <a href="#">step 31</a>

## 20

The port connection conflicts with the configured port type. Either an expansion port (E\_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F\_Port) is incorrectly cabled to a fabric element (director or switch).

1. At the Hardware View, click **Configure > Ports**. The Configure Ports dialog box displays.
2. Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.
3. Click the **Type** field and configure the port from the list box as follows:
  - Click fabric port (**F\_Port**) if the port is cabled to a device (node).

- Click expansion port (**E\_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.

4. Click **Activate** to save the configuration information and close the dialog box.

Did reconfiguring the port type solve the problem?

**NO**                      **YES**

↓

The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

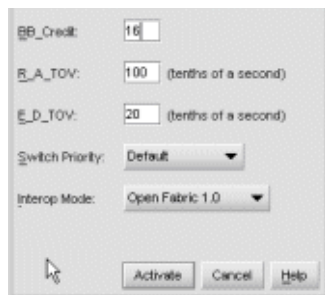
## 21

One of the following mode-mismatch conditions was detected and an ISL connection is not allowed:

- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a legacy HP director or switch at the incorrect Exchange Link Parameter (ELP) revision level.
- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a non-HP switch at the incorrect ELP revision level.
- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a non-HP switch.

Reconfigure the director operating mode:

1. Ensure the director is set offline (“[Set Offline State](#)” on page 206).
2. At the Hardware View, click **Configure > Operating Parameters > Fabric Parameters**. The Configure Fabric Parameters dialog box displays, as shown in [Figure 29](#) on page 129.



**Figure 29: Fabric Parameters dialog box**



3. Select the operating mode by clicking one of the following options on the **Interop Mode** drop-down list:

- **Open Fabric 1.0**
- **Homogeneous**

4. Click **Activate** to save the selection and close the window.

Did configuring the operating mode solve the problem?

**NO**                      **YES**

↓                      The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 22

A loopback plug is connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

**YES**                      **NO**

↓                      Contact the next level of support. **Exit MAP.**

---

## 23

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the director.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is **No Light**.
- If the port is operational and a device is attached, the green LED illuminates, the amber LED extinguishes, and the port state is **Online**.

Did removing the loopback plug solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 24

A port connection timed out because of an unresponsive device (node) or an ISL connection was not allowed because of a security violation (authorization failure reject). Check the port status and clean the fiber-optic connectors on the cable.

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port ("Block a Port" on page 207).
3. Disconnect both ends of the fiber optic cable.
4. Clean the fiber optic connectors. ("Clean Fiber Optic Components" on page 199).
5. Reconnect the fiber optic cable.
6. Unblock the port ("Unblock a Port" on page 209).
7. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES**            **NO**

↓            The Fibre Channel link and director are operational. **Exit MAP.**

---

## 25

Inspect both SBAR assemblies at the rear of the director. SBAR assembly LEDs can be inspected through the hexagonal cooling vents of the RFI shield.

Is the amber LED on an SBAR assembly illuminated but not blinking (beaconing)?

**YES**            **NO**

↓            The director is operational. Go to [step 27](#).

---

## 26

An SBAR assembly failed and must be removed and replaced (“[RRP: Redundant SBAR Assembly](#)” on page 248).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did SBAR assembly replacement solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 27

Inspect and service the host bus adapters (HBAs), as necessary.

Did service of the HBAs solve the problem?

**NO**            **YES**

↓            **Exit MAP.**

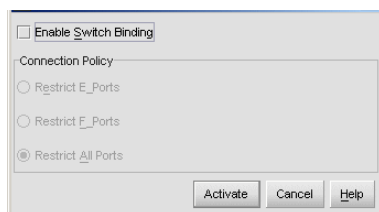
Contact the next level of support. **Exit MAP.**

---

## 28

A port connection is not allowed because of an Exchange Security Attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements.

1. At the Hardware View, click **Configure > Switch Binding > Change State**. The Switch Binding - State Change dialog box displays, as shown in [Figure 30](#).



**Figure 30: Switch Binding - State Change dialog box**

2. Ensure the **Enable Switch Binding** check box is enabled (checked) for both directors.
3. Ensure the **Connection Policy** radio buttons are compatible for both directors.
4. Click **Activate** for each director or switch. The switch binding feature is consistently enabled for both directors or switches.

Did configuring the switch binding parameters solve the problem?

**NO**                      **YES**



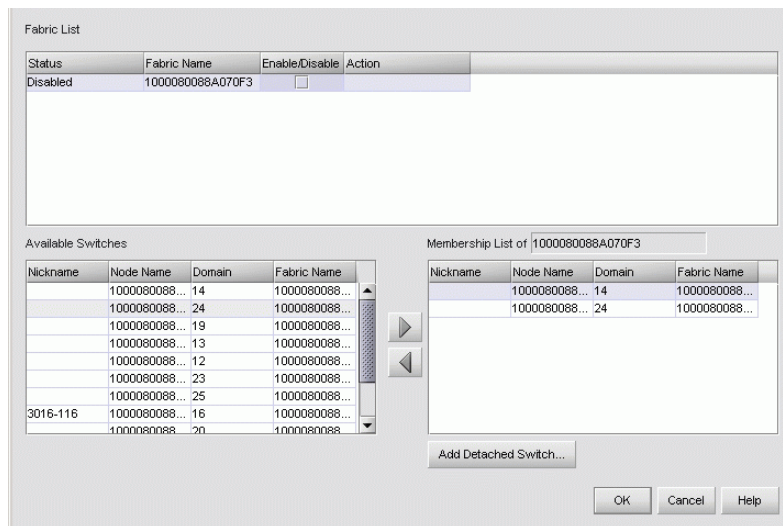
The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 29

A port connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both fabric elements.

1. At the HAFM main window, click **Configure > Fabric Binding**. The Fabric Binding dialog box displays, as shown in [Figure 31](#).



**Figure 31: Fabric Binding dialog box**

2. At the **Fabric List** section, ensure the **Enable/Disable** check box is enabled (checked) for the fabric containing both directors or switches.

- At the **Membership List of <Fabric Name>** section, update the membership list for both elements to ensure interswitch compatibility, then click **OK**. The fabric binding feature is consistently enabled for both directors or switches.

Did updating the fabric membership lists solve the problem?

**NO**                      **YES**



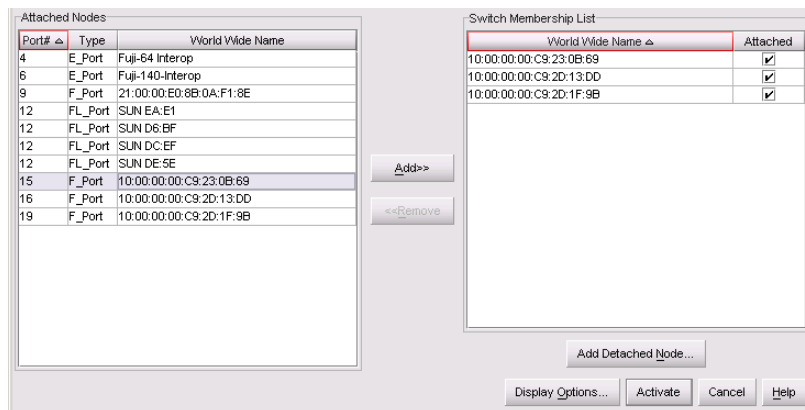
The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 30

A port connection is not allowed because of a switch binding mismatch. Switch membership lists must be compatible for both fabric elements.

- At the Hardware View for each director or switch, click **Configure > Switch Binding > Edit Membership List**. The Switch Binding - Membership List dialog box displays, as shown in [Figure 32](#).



**Figure 32: Switch Binding - Membership List dialog box**

- Ensure the **Switch Membership List** is updated and correct for each director or switch.
- Click **Activate** for each director or switch. The switch binding feature is consistently enabled for both directors or switches.

Did updating the switch membership lists solve the problem?

**NO**            **YES**

↓            The director is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 31

A port connection is not allowed because of a Computer Network Technologies (CNT) wide area network (WAN) extension mode mismatch. Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a director set to CNT WAN extension mode.

Contact Computer Network Technologies for support. **Exit MAP.**

---

## 32

The director and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

**NO**            **YES**

↓            The Fibre Channel link and director are operational. **Exit MAP.**

Go to [step 1](#).

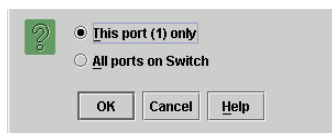
---

## 33

A link incident message displayed in the Link Incident Log or in the **Link Incident** field of the Port Properties dialog box; or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI or FICON server attached to the director reporting the problem.

Clear the link incident for the port.

1. At the Hardware View, right-click the port. A menu displays.
2. Click **Open Port Card View**. The Port Card View displays.
3. Right-click the port. A menu displays
4. Click **Clear Link Incident Alert(s)**. The Clear Link Incident Alert(s) dialog box displays, as shown in [Figure 33](#).



**Figure 33: Clear Link Incident Alert(s) dialog box**

5. Make sure the **This port (n) only** option (where n is the port number) is selected and click **OK**. The link incident clears.
6. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES**            **NO**



The problem is transient and the Fibre Channel link and director are operational. **Exit MAP.**

---

## 34

Inspect the fiber optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port ("[Block a Port](#)" on page 207).
3. Remove and replace the fiber optic jumper cable.
4. Unblock the port ("[Unblock a Port](#)" on page 209).

Was a corrective action performed?

**YES**            **NO**



Go to [step 36](#).

---

## 35

Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES**            **NO**



The Fibre Channel link and director are operational. **Exit MAP.**

---

**36**

Clean fiber optic connectors on the jumper cable.

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port (“[Block a Port](#)” on page 207).
3. Disconnect both ends of the fiber optic jumper cable.
4. Clean the fiber optic connectors (“[Clean Fiber Optic Components](#)” on page 199).
5. Reconnect the fiber optic jumper cable.
6. Unblock the port (“[Unblock a Port](#)” on page 209).
7. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES**

**NO**

↓

The Fibre Channel link and director are operational. **Exit MAP.**

---

**37**

Disconnect the fiber optic jumper cable from the director port and connect the cable to a spare port.

Is a link incident reported at the new port?

**YES**

**NO**

↓

Go to [step 39](#).



---

## 38

The attached device is causing the recurrent link incident. Notify the customer of the problem and have the system administrator:

1. Inspect and verify operation of the attached device.
2. Repair the attached device if a failure is indicated.
3. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES**            **NO**

↓

The attached device, Fibre Channel link, and director are operational.  
**Exit MAP.**

---

## 39

The director port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port or UPM card degradation and a possible pending failure. Go to [step 6](#).

---

## 40

A UPM card is not recognized by director firmware because the firmware version is not supported or the UPM card failed. Advise the customer of the problem and determine the correct firmware version to download from the HAFM appliance.

Download the firmware (“[Download a Firmware Version to a Director](#)” on page 215). Perform the data collection procedure after the download. **Continue.**

---

## 41

Did the firmware download solve the problem?

**NO**            **YES**

↓

The director is operational. **Exit MAP.**

A UPM card failure is indicated. Go to [step 7](#).

---

## 42

Is the Embedded Web Server interface operational?

**NO**            **YES**

↓

Go to [step 45](#).

---

---

## 43

A Page cannot be found, Unable to locate the server, HTTP 404-file not found, or other similar message displays. The message indicates the Web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP2 cards failed.

**Continue.**

---

## 44

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP2 card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

**YES**

**NO**



Analysis for an Ethernet link, AC power distribution, or dual CTP2 card failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**

---

## 45

Inspect UPM card operational states at the Embedded Web Server interface.

1. At the View panel, click the **FRU Properties** tab. The View panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for UPM cards. Scroll down the View panel as necessary.

Does the **Status** field display a **Failed** message for a UPM card?

**NO**                      **YES**

↓                      A UPM card failure is indicated. Go to [step 7](#).

## 46

Inspect Fibre Channel port operational states at the Embedded Web Server interface.

1. At the View panel, click the **Port Properties** tab. The View panel (**Port Properties** tab) displays with port **0** highlighted in red.
2. Click the port number (**0** through **63**) for which a failure is suspected to display properties for that port.
3. Inspect the **Operational State** field. Scroll down the View panel as necessary.
4. [Table 15](#) lists port operational states and associated MAP 0600 steps that describe fault isolation procedures.

**Table 15: MAP 0600: Port Operational States and Actions**

Operational State	Action
Offline	Go to <a href="#">step 16</a>
Not Operational	Go to <a href="#">step 16</a>
Port Failure	Go to <a href="#">step 6</a>
Testing	Internal or external loopback test in process. Exit MAP.
Invalid Attachment	Go to <a href="#">step 18</a>
Link Reset	Go to <a href="#">step 32</a>
Not Installed	Go to <a href="#">step 47</a>

## 47

Install an SFP optical transceiver in the port receptacle (“[RRP: SFP Optical Transceiver](#)” on page 241).

1. This procedure is concurrent and can be performed while director power is on.
2. Verify location of the uninstalled port transceiver.
  - For an OSI environment, [Figure 34](#) and [Figure 35](#) page 140 show UPM card numbers (**0** through **15**) and port numbers (**00** through **63**).
  - For a FICON environment, [Figure 34](#) and [Figure 35](#) show UPM card numbers (**0** through **15**), port numbers (**00** through **63**), and bolded logical port addresses (hexadecimal **04** through **43**).
3. Perform an external loopback test for the port as part of FRU removal and replacement. **Exit MAP.**

UPM Cards								CTP2 - 1 Card	CTP2 - 0 Card	UPM Cards							
15	14	13	12	11	10	9	8			7	6	5	4	3	2	1	0
63	59	55	51	47	43	39	35			31	27	23	19	15	11	07	03
62	58	54	50	46	42	38	34			30	26	22	18	14	10	06	02
61	57	53	49	45	41	37	33			29	25	21	17	13	09	05	01
60	56	52	48	44	40	36	32			28	24	20	16	12	08	04	00

**Figure 34: UPM card diagram (OSI)**

UPM Cards								CTP2 - 1 Card	CTP2 - 0 Card	UPM Cards							
15	14	13	12	11	10	9	8			7	6	5	4	3	2	1	0
<b>43</b>	<b>3F</b>	<b>3B</b>	<b>37</b>	<b>33</b>	<b>2F</b>	<b>2B</b>	<b>27</b>			<b>23</b>	<b>1F</b>	<b>1B</b>	<b>17</b>	<b>13</b>	<b>0F</b>	<b>0B</b>	<b>07</b>
63	59	55	51	47	43	39	35			31	27	23	19	15	11	07	03
<b>42</b>	<b>3E</b>	<b>3A</b>	<b>36</b>	<b>32</b>	<b>2E</b>	<b>2A</b>	<b>26</b>			<b>22</b>	<b>1E</b>	<b>1A</b>	<b>16</b>	<b>12</b>	<b>0E</b>	<b>0A</b>	<b>06</b>
62	58	54	50	46	42	38	34			30	26	22	18	14	10	06	02
<b>41</b>	<b>3D</b>	<b>39</b>	<b>35</b>	<b>31</b>	<b>2D</b>	<b>29</b>	<b>25</b>			<b>21</b>	<b>1D</b>	<b>19</b>	<b>15</b>	<b>11</b>	<b>0D</b>	<b>09</b>	<b>05</b>
61	57	53	49	45	41	37	33			29	25	21	17	13	09	05	01
<b>40</b>	<b>3C</b>	<b>38</b>	<b>34</b>	<b>30</b>	<b>2C</b>	<b>28</b>	<b>24</b>			<b>20</b>	<b>1C</b>	<b>18</b>	<b>14</b>	<b>10</b>	<b>0C</b>	<b>08</b>	<b>04</b>
60	56	52	48	44	40	36	32			28	24	20	16	12	08	04	00

**Figure 35: UPM card diagram (FICON)**

## MAP 0700: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes isolation of fabric logout, interswitch link (ISL), and E\_Port segmentation problems. Failure indicators include:

- An event code recorded at the Director 2/64 Event Log or the Embedded Web Server Event Log.
- A segmentation reason associated with a Fibre Channel port at the Embedded Web Server interface.
- A yellow triangle (attention indicator) displays over a UPM card graphic or at the alert panel of the Hardware View.
- A link incident message recorded in the Link Incident Log or Port Properties dialog box.

### 1

Was an event code **010, 011, 020, 021, 050, 051, 052, 060, 061, 062, 063, 070, 071, 072, 140, 142, or 150** observed at the Director 2/64 Event Log (HAFM appliance) or at the Embedded Web Server Event Log?

**YES**

**NO**



Go to [step 3](#).

### 2

[Table 16](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 16: MAP 0700: Event Codes**

Event Code	Explanation	Action
010	Login server unable to synchronize databases.	Go to <a href="#">step 7</a>
011	Login server database invalid.	Go to <a href="#">step 7</a>
020	Name server unable to synchronize databases.	Go to <a href="#">step 7</a>
021	Name server database invalid.	Go to <a href="#">step 7</a>
050	HAFM appliance unable to synchronize databases.	Go to <a href="#">step 8</a>
051	HAFM appliance database invalid.	Go to <a href="#">step 8</a>
052	HAFM appliance internal error.	Go to <a href="#">step 8</a>

**Table 16: MAP 0700: Event Codes (Continued)**

Event Code	Explanation	Action
060	Fabric controller unable to synchronize databases.	Go to <a href="#">step 9</a>
061	Fabric controller database invalid.	Go to <a href="#">step 9</a>
062	Maximum interswitch hop count exceeded.	Go to <a href="#">step 10</a>
063	Received link state record too large.	Go to <a href="#">step 11</a>
070	E_Port is segmented.	Go to <a href="#">step 12</a>
071	Director is isolated.	Go to <a href="#">step 12</a>
072	E_Port connected to unsupported switch.	Go to <a href="#">step 13</a>
140	Congestion detected on an ISL.	Go to <a href="#">step 21</a>
142	Low BB_Credit detected on an ISL.	Go to <a href="#">step 26</a>
150	Zone merge failure.	Go to <a href="#">step 27</a>

### 3

Is fault isolation being performed at the HAFM appliance?

**YES**      **NO**



Fault isolation is being performed through the Embedded Web Server interface. Go to [step 26](#).

### 4

Does a yellow triangle (attention indicator) display over a UPM card graphic at the Hardware View?

**YES**      **NO**



The problem is transient and the director-to-fabric element connection is operational. **Exit MAP.**

## 5

Inspect the port state and LED status for all ports with an attention indicator.

1. At the Hardware View, double-click the port with the attention indicator. The Port card View displays
2. Double-click the port with the attention indicator. The Port Properties dialog box displays.
3. Inspect the **Operational State** field in the Port Properties dialog box.

Does the **Operational State** field indicate **Segmented E\_Port**?

**YES**      **NO**



Analysis for a UPM card failure or other link incident is not described in this MAP. Go to “[MAP 0600: UPM Card Failure and Link Incident Analysis](#)” on page 118. **Exit MAP.**

## 6

Inspect the **Segmentation Reason** field at the Port Properties dialog box. [Table 17](#) lists port segmentation reasons and associated steps that describe fault isolation procedures.

**Table 17: MAP 0700: Segmentation Reasons and Actions**

Segmentation Reason	Action
Incompatible operating parameters.	Go to <a href="#">step 14</a>
Duplicate domain IDs.	Go to <a href="#">step 15</a>
Incompatible zoning configurations.	Go to <a href="#">step 16</a>
Build fabric protocol error.	Go to <a href="#">step 17</a>
No principal switch.	Go to <a href="#">step 19</a>
No response from attached switch.	Go to <a href="#">step 20</a>
ELP retransmission failure timeout.	Go to <a href="#">step 21</a>

## 7

A minor error occurred that caused fabric services databases to be reinitialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the errors.

- **Event code 010**—Following a CTP2 card reset, the login server attempted to acquire a fabric server database copy from the other CTP2 card and failed.
- **Event code 011**—Following a CTP2 card failover, the login server database failed cyclic redundancy check (CRC) validation.
- **Event code 020**—Following a CTP2 card reset, the name server attempted to acquire a fabric server database copy from the other CTP2 card and failed.
- **Event code 021**—Following CTP2 card failover, the name server database failed CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the backup CD to HP for analysis by third-level support personnel. **Exit MAP.**

---

## 8

A minor error occurred that caused HAFM appliance databases to be reinitialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the errors.

- **Event code 050**—Following CTP2 card reset, the HAFM appliance attempted to acquire a database copy from the other CTP2 card and failed.
- **Event code 051**—Following CTP2 card failover, the HAFM appliance database failed CRC validation.
- **Event code 052**—An internal operating error was detected by the HAFM appliance subsystem.

All attached devices resume operation after HAFM appliance login. Perform the data collection procedure and return the backup CD to HP for analysis by third-level support personnel. **Exit MAP.**



---

## 9

A minor error occurred that caused fabric controller databases to be reinitialized to an empty state. As a result, the director briefly lost interswitch link capability. The following list explains the errors.

- **Event code 060**—Following CTP2 card reset, the fabric controller attempted to acquire a database copy from the other CTP2 card and failed.
- **Event code 061**—Following CTP2 card failover, the fabric controller database failed CRC validation.

All interswitch links resume operation after CTP2 card reset or failover. Perform the data collection procedure and return the backup CD to HP for analysis by third-level support personnel. **Exit MAP.**

---

## 10

As indicated by an event code **062**, the fabric controller software detected a path to another director (or fabric element) in a multi-switch fabric that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

**NO**                      **YES**

↓

The director and multi-switch fabric are operational.  
**Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 11

As indicated by an event code **063**, the fabric controller software detected a fabric element (director or switch) in a multi-switch fabric that has more than 32 ISLs attached. Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no director or switch elements have more than 32 ISLs.

Did fabric reconfiguration solve the problem?

**NO YES**

↓ The director and multi-switch fabric are operational. **Exit MAP.**  
Contact the next level of support. **Exit MAP.**

## 12

A **070** event code indicates an E\_Port detected an incompatibility with an attached director and prevented the directors from forming a multi-switch fabric. A segmented E\_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the director is isolated from all directors in a multi-switch fabric, and is accompanied by a **070** event code for each segmented E\_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

1. At the Hardware View, click **Logs > Event Log**. The Event Log displays.
2. Examine the first five bytes (**0** through **4**) of event data.
3. Byte **0** specifies the director port number (**00** through **63**) of the segmented E\_port. Byte **4** specifies the segmentation reason (Table 18).

**Table 18: MAP 0700: Byte 4, Segmentation Reasons**

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to <a href="#">step 14</a>
02	Duplicate domain IDs.	Go to <a href="#">step 15</a>
03	Incompatible zoning configurations.	Go to <a href="#">step 16</a>
04	Build fabric protocol error.	Go to <a href="#">step 17</a>
05	No principal switch.	Go to <a href="#">step 19</a>
06	No response from attached switch.	Go to <a href="#">step 20</a>
07	ELP retransmission failure timeout.	Go to <a href="#">step 21</a>

## 13

As indicated by an event code **072**, a director E\_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. **Exit MAP.**

---

## 14

A director E\_Port segmented because the error detect time out value (E\_D\_TOV) or resource allocation time-out value (R\_A\_TOV) is incompatible with the attached fabric element.

1. Contact HP customer support or engineering personnel to determine the recommended E\_D\_TOV and R\_A\_TOV values for both directors.
2. Notify the customer that both directors will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the directors and sets attached devices offline.
3. Set both directors offline (“[Set Offline State](#)” on page 206).
4. At the Hardware View for the first director reporting the problem, click **Configure > Operating Parameters > Fabric Parameters**. The Configure Fabric Parameters dialog box displays, as shown in [Figure 29](#) on page 129.
5. Type the recommended E\_D\_TOV and R\_A\_TOV values, then click **Activate**.
6. Repeat [step 4](#) and [step 5](#) at the Hardware View for the director attached to the segmented E\_Port (second director). Use the same E\_D\_TOV and R\_A\_TOV values.
7. Set both directors online (“[Set Online State](#)” on page 205).

Did the operating parameter change solve the problem, and did both directors join through the ISL to form a fabric?

**NO**

**YES**

↓

The directors, associated ISL, and multi-switch fabric are operational.  
**Exit MAP.**

Contact the next level of support. **Exit MAP.**

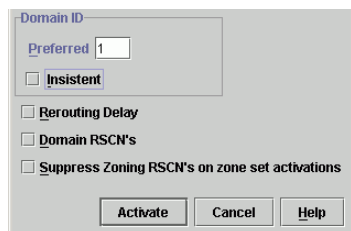
---

## 15

A director E\_Port segmented because two fabric elements had duplicate domain IDs.

1. Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each director.
2. Notify the customer that both directors will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the directors and sets attached devices offline.

3. Set both directors offline (“[Set Offline State](#)” on page 206).
4. At the Hardware View for the first director reporting the problem, click **Configure > Operating Parameters > Switch Parameters**. The Configure Switch Parameters dialog box displays, as shown in [Figure 36](#).



**Figure 36: Configure Switch Parameters dialog box**

5. Type the customer-determined preferred domain ID value, then click **Activate**.
6. Repeat [step 4](#) and [step 5](#) at the Hardware View for the director attached to the segmented E\_Port (second director). Use a different preferred domain ID value.
7. Set both directors online (“[Set Online State](#)” on page 205).

Did the domain ID change solve the problem, and did both directors join through the ISL to form a fabric?

**NO**                      **YES**

↓

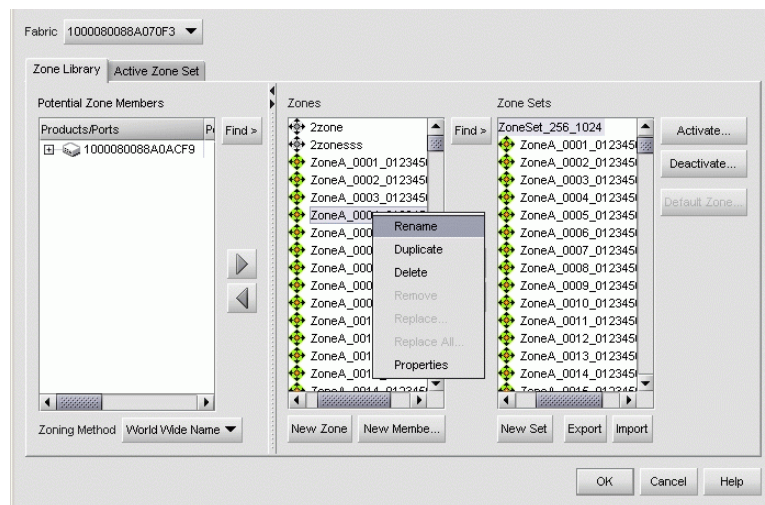
The directors, associated ISL, and multi-switch fabric are operational.  
**Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 16

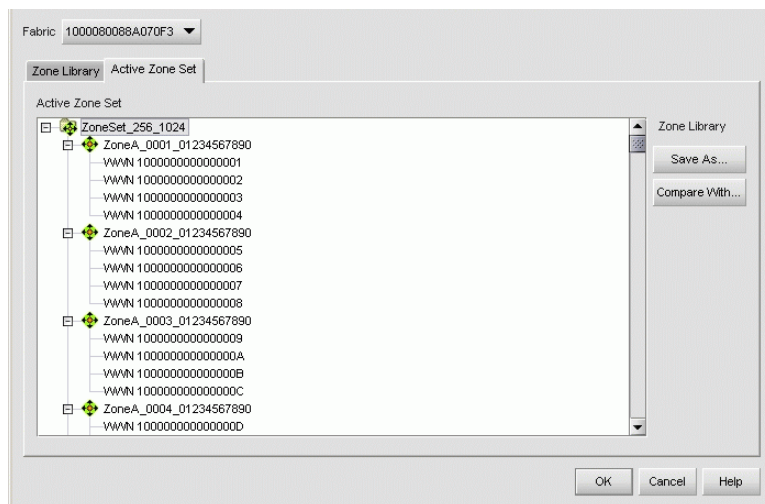
A director E\_Port segmented because two directors had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both directors, but the zones contain different members.

1. Work with the system administrator to determine the desired zone name change for one of the affected directors. Zone names must conform to the following rules:
  - The name must be 64 characters or fewer in length.
  - The first character must be a letter (**a** through **z**), upper or lowercase.
  - Other characters are alphanumeric (**a** through **z** or **0** through **9**), dollar sign (\$), hyphen (-), caret (^), or underscore (\_).
2. Close the Element Manager (Hardware View). The HAFM main window displays.
3. At the HAFM main window physical map, right-click the blue background representing the fabric containing the switch reporting the problem. A pop-up menu displays.
4. Click **Zoning**. The Zoning dialog box displays with the Zone Library page open, as shown in [Figure 37](#).



**Figure 37: Zoning dialog box (Zone Library tab)**

5. Click the **Active Zone Set** tab. The Zoning dialog box displays with the Active Zone Set page open, as shown in [Figure 38](#).



**Figure 38: Zoning dialog box (Active Zone Set tab)**

6. Inspect zone names in the active zone set to determine the incompatible name.
7. Modify the incompatible zone name as directed by the customer:
  - a. At the Zoning dialog box, click the **Zone Library** tab. The dialog box returns to the Zone Library page, as shown in [Figure 37](#) on page 149.
  - b. Right-click the zone name to be changed from the **Zones** field. A pop-up menu displays.
  - c. Click **Rename**. The selected zone name remains highlighted in blue.
  - d. Enter the new zone name (specified by the customer).
  - e. Click **OK** to activate the change and close the Zoning dialog box.

Did the zone name change solve the problem, and did both directors join through the ISL to form a fabric?

**NO**                      **YES**

↓

The directors, associated ISL, and multi-switch fabric are operational.  
**Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 17

A director E\_Port segmented because a build fabric protocol error was detected.

1. Disconnect the fiber optic jumper cable from the segmented E\_Port.
2. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both directors join through the ISL to form a fabric?

**NO**                      **YES**

↓

The directors, associated ISL, and multi-switch fabric are operational.  
**Exit MAP.**

---

## 18

Initial program load (IPL) the director (“[TML, IPL, or Reset the Director](#)” on page 202).

Did the IPL solve the problem and did both directors join through the ISL to form a fabric?

**NO**                      **YES**

↓

The directors, associated ISL, and multi-switch fabric are operational.  
**Exit MAP.**

Perform the data collection procedure and contact the next level of support. **Exit MAP.**

---

## 19

A director E\_Port segmented because no director in the fabric is capable of becoming the principal switch.

1. Notify the customer the director will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline (“[Set Offline State](#)” on page 206).
3. At the Hardware View for the director, click **Configure > Operating Parameters > Switch Parameters**. The Configure Switch Parameters dialog box displays, as shown in [Figure 36](#) on page 148.

4. At the **Switch Priority** field, select a switch priority (**Principal**, **Never Principal**, or **Default**). The switch priority value designates the fabric's principal switch. The principal switch is assigned a priority of 1 and controls the allocation and distribution of domain IDs for all fabric directors and switches (including itself).

**Principal** is the highest priority setting, **Default** is the next highest, and **Never Principal** is the lowest priority setting. The setting **Never Principal** means that the switch is incapable of becoming a principal switch. If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a multi-switch fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all ISLs segment and the message "No Principal Switch" displays in the **Reason** field of the Port Properties dialog box.

5. Set the director online ("[Set Online State](#)" on page 205).

Did the switch priority change solve the problem and did both directors join through the ISL to form a fabric?

**NO**                      **YES**



The directors, associated ISL, and multi-switch fabric are operational.  
**Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 20

A director E\_Port segmented (at an operational director) because a response to a verification check indicates an attached director is not operational.

1. Perform the data collection procedure at the operational director and return the backup CD to HP for analysis by third-level support personnel.
2. Go to "[MAP 0000: Start MAP](#)" on page 46 and perform fault isolation for the failed director.

**Exit MAP.**



## 21

A **140** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

No action is required for an isolated event. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the directors or switches reporting the problem.
- Increase the ISL link speed between the directors or switches reporting the problem (from 1 Gb/s to 2 Gb/s).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported ISL congestion?

**NO**                      **YES**

↓                      The ISL is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

---

## 22

A **142** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with no transmission BB\_Credit for a period of time that exceeded the configured low BB\_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the directors or switches reporting the problem.
- Increase the ISL link speed between the directors or switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported low BB\_Credit condition?

**NO**                      **YES**

↓                      The ISL is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 23

A **150** event code indicates a zone merge failed during ISL initialization. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a **070** event code, and represents the reply of an adjacent fabric element in response to a zone merge frame.

Obtain supplementary event data for each **150** event code.

1. At the Hardware View, click **Logs > Event Log**. The Event Log displays.
2. Examine the first 12 bytes (**0** through **11**) of event data.
3. Bytes **0** through **3** specify the E\_Port number (**00** through **23**) reporting the problem. Bytes **8** through **11** specify the failure reason ([Table 19](#)).

**Table 19: Bytes 8 through 11 Failure Reasons and Actions**

Bytes 8 - 11	Failure Reason	Action
01	Invalid data length.	Go to <a href="#">step 24</a>
08	Invalid zone set format.	Go to <a href="#">step 24</a>
09	Invalid data.	Go to <a href="#">step 25</a>
0A	Cannot merge.	Go to <a href="#">step 25</a>
F0	Retry limit reached.	Go to <a href="#">step 24</a>
F1	Invalid response length.	Go to <a href="#">step 24</a>
F2	Invalid response code.	Go to <a href="#">step 24</a>

---

## 24

A zone merge failed during ISL initialization. The following list explains the reason:

- **Failure reason 01**—An invalid data length condition caused an error in a zone merge frame.
- **Failure reason 08**—An invalid zone set format caused an error in a zone merge frame.
- **Failure reason F0**—A retry limit reached condition caused an error in a zone merge frame.
- **Failure reason F1**—An invalid response length condition caused an error in a zone merge frame.
- **Failure reason F2**—An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E\_Port reporting the problem, then reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem, and was the resulting zone merge successful?

**NO**                      **YES**

↓

The merged zone is operational. **Exit MAP.**

Perform the data collection procedure and return the CD to HP for analysis. Contact the next level of support. **Exit MAP.**

---

## 25

A zone merge failed during ISL initialization. The following list explains the reason:

- **Failure reason 09**—Invalid data caused a zone merge failure.
- **Failure reason 0A**—A Cannot Merge condition caused a zone merge failure.

Obtain supplementary error code data for the **150** event code.

1. At the Hardware View, click **Logs > Event Log**. The Event Log displays.
2. Examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform the data collection procedure and return the CD to HP for analysis. Contact the next level of support, and report the **150** event code, the associated failure reason, and the associated error code. **Exit MAP.**

---

**26**

Is the Embedded Web Server interface operational?

**YES**      **NO**



Analysis for an Ethernet link, AC power distribution, or CTP2 card failure is not described in this MAP. Go to “[MAP 0000: Start MAP](#)” on page 46. If this is the second time at this step, contact the next level of support. **Exit MAP.**

---

**27**

Inspect the Fibre Channel port segmentation reason at the Embedded Web Server interface.

1. At the View panel, click the **Port Properties** tab. The View panel (**Port Properties** tab) displays.
2. Click the port number (**0** through **63**) of the segmented port.
3. Inspect the **Segmentation Reason** field for the selected port.

Is the **Segmentation Reason** field blank or does it display an N/A message?

**NO**      **YES**



The director ISL is operational. **Exit MAP.**

The **Segmentation Reason** field displays a message. [Table 20](#) lists segmentation reasons and associated steps that describe fault isolation procedures.

**Table 20: MAP 0700: Segmentation Reasons and Actions**

Segmentation Reason	Action
Incompatible operating parameters.	Go to <a href="#">step 14</a>
Duplicate domain IDs.	Go to <a href="#">step 15</a>
Incompatible zoning configurations.	Go to <a href="#">step 16</a>
Build fabric protocol error.	Go to <a href="#">step 17</a>
No principal switch.	Go to <a href="#">step 19</a>
No response from attached switch.	Go to <a href="#">step 20</a>
ELP retransmission failure timeout.	Go to <a href="#">step 21</a>

## MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination

This MAP describes isolation of hardware-related problems with the HAFM appliance platform. Although this MAP provides high-level fault isolation instructions, refer to the documentation provided with the HAFM appliance for detailed problem determination and resolution.

---

### 1

Are you performing fault isolation at a customer-supplied server communicating with the director through the EWS interface?

**NO**                      **YES**



The server and Internet browser application are not HP-supported, and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions to resolve the problem. **Exit MAP.**

---

### 2

Are you performing fault isolation at a customer-supplied, UNIX® based server running the client *HAFM* application?

**NO**                      **YES**



UNIX-based servers are not HP-supported, and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions to resolve the problem. **Exit MAP.**

---

### 3

Are you performing fault isolation at one of the following?

- The HAFM appliance running the Windows 2000 Professional operating system.
- A customer-supplied server running the client *HAFM* application and a Windows operating system (Windows 95, Windows 98, Windows 2000, Windows XP, or Windows NT® 4.0).

**YES**                      **NO**



Analysis for the appliance or server failure is not described in this MAP. Contact the next level of support. **Exit MAP.**

---

## 4

At the HAFM appliance, close the *HAFM* application.

1. At the HAFM main window, click **SAN > Exit**. The *HAFM* application closes.
2. Close any other applications that are running.

**Continue.**

---

## 5

Inspect the available random access memory (RAM). The computer must have a minimum of 128 megabytes (MB) of memory to run the Windows 2000 operating system and *HAFM* application.

1. Right-click anywhere in the **Windows 2000** task bar at the bottom of the desktop. A menu displays.
2. Click **Task Manager**. The Windows 2000 Task Manager dialog box displays with the Applications page open. Click **Performance** to open the Performance page.
3. At the **Physical Memory (K)** portion of the dialog box, inspect the total amount of physical memory.
4. Close the dialog box.

Does the computer have sufficient memory?

**YES**

**NO**

↓

A memory upgrade is required. Inform the customer of the problem and contact the next level of support. **Exit MAP.**

---

## 6

Reboot the HAFM appliance and perform system diagnostics.

1. Click **Start > Shut Down**. The Shut Down Windows dialog box displays.
2. Click **Shut down** on the drop-down list and then click **OK** to power off the HAFM appliance.
3. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the server and perform power-on self-tests (POSTs). During POSTs:
  - a. The green LCD panel illuminates.

- b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
- c. After a few seconds, the LCD panel displays a message, as shown in [Figure 8](#) on page 48.
- d. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - Central processing unit (CPU) temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
4. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays HAFM appliance operational information.
5. After rebooting the HAFM appliance at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. The *HAFM* application starts and the HAFM 8 Log In dialog box displays, as shown in [Figure 9](#) on page 49.

Did POSTs detect a problem?

**NO**                      **YES**



A computer hardware problem exists. Refer to the supporting documentation shipped with the HAFM appliance for instructions on resolving the problem. **Exit MAP.**

---

## 7

After rebooting the HAFM appliance, the HAFM Services and *HAFM* applications start, and the HAFM 8 Log In dialog box displays.

Did the HAFM 8 Log In dialog box display?

**YES**

**NO**



Go to [step 9](#).

---

## 8

Log in to the HAFM appliance using the HAFM 8 Log In dialog box.

1. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*.

The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.

If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.

2. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
3. If you want your computer to save the login information, click the **Save Password** option.
4. Click **Login**. The View All - HAFM 8 window displays, as shown in [Figure 10](#) on page 50.

Did the View All - HAFM 8 window display and is the *HAFM* application operational?

**NO**

**YES**



The HAFM appliance is operational. **Exit MAP.**



## 9

Perform one of the following:

- If the HAFM appliance has standalone diagnostic test programs resident on the hard drive, perform the diagnostics. Refer to supporting documentation shipped with the HAFM appliance for instructions.
- If the HAFM appliance does not have standalone diagnostic test programs resident on hard drive, go to [step 10](#).

Did diagnostic test programs detect a problem?

**NO**

**YES**

↓

Refer to the supporting documentation shipped with the HAFM appliance for instructions to resolve the problem. **Exit MAP.**

---

## 10

Reboot the HAFM appliance.

1. Click **Start > Shut Down**. The Shut Down Windows dialog box displays.
2. Click **Shut down** on the drop-down list and then click **OK** to power off the HAFM appliance.
3. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the server and perform power-on self-tests (POSTs). During POSTs:
  - a. The green LCD panel illuminates.
  - b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  - c. After a few seconds, the LCD panel displays a message, as shown in [Figure 8](#) on page 48.
  - d. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
    - Host name.
    - System date and time.
    - LAN 1 and LAN 2 IP addresses.
    - Fan 1, fan 2, fan 3, and fan 4 rotational speed.

- Central processing unit (CPU) temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
4. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays server operational information.
  5. After rebooting the server at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. The *HAFM* application starts and the HAFM 8 Log In dialog box displays, as shown in [Figure 9](#) on page 49.
  6. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*.  
The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.  
If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.
  7. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
  8. If you want your computer to save the login information, click **Save Password**.
  9. Click **Login**. The View All - HAFM 8 window displays, as shown in [Figure 10](#) on page 50.

Did the View All - HAFM 8 window display and is the *HAFM* application operational?

**NO**            **YES**

↓            The HAFM appliance is operational. **Exit MAP.**

---

## 11

Re-install the *HAFM* application (“[Install or Upgrade Software](#)” on page 223).

Did the *HAFM* application install and open successfully?

**NO**            **YES**

↓            The HAFM appliance is operational. **Exit MAP.**

---

## 12

Advise the customer and next level of support that the HAFM appliance hard drive should be restored to its original factory configuration. If the customer and support personnel do not concur, go to [step 13](#).

1. Format the server hard drive. Refer to supporting documentation shipped with the server for instructions.
2. Restore the HAFM appliance hard drive using the *HAFM appliance Restore/Boot CD* shipped with the HAFM appliance. Refer to the *readme.txt* file on the CD for instructions.
3. Install the *HAFM* application.

Did the HAFM appliance hard drive format, and did the operating system and *HAFM* application install and open successfully?

**NO**            **YES**

↓            The HAFM appliance is operational. **Exit MAP.**

---

## 13

Additional analysis for the failure is not described in this MAP. Contact the next level of support. **Exit MAP.**



# Repair Information

## 3

This chapter describes repair and repair-related procedures used by service representatives for the Director 2/64 and associated field-replaceable units (FRUs). The procedures are performed using one of the following:

- *HAFM* application
- Director 2/64 Element Manager
- Embedded Web Server (EWS)

The following procedures are described in this chapter:

- [Using Log Information](#), page 167
- [Obtaining Port Diagnostic Information](#), page 170
- [Collecting Maintenance Data](#), page 197
- [Clean Fiber Optic Components](#), page 199
- [Power-On Procedure](#), page 200
- [Power-Off Procedure](#), page 201
- [IML, IPL, or Reset the Director](#), page 202
- [Set the Director Online or Offline](#), page 205
- [Block and Unblock Ports](#), page 207
- [Manage Firmware Versions](#), page 211
- [Manage Configuration Data](#), page 218
- [Install or Upgrade Software](#), page 223

Do not perform repairs until a failure is isolated to an FRU. If fault isolation was not performed, go to “[MAP 0000: Start MAP](#)” on page 46.

## Factory Defaults

**Table 21** lists the defaults for the passwords and IP, subnet, and gateway addresses.

**Table 21: Factory-set Defaults**

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Procedural Notes

---

**Note:** HAFM and Element Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed, and the fields may contain data that does not match the data seen on your system.

---

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a repair procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all electrostatic discharge (ESD) procedures, **WARNING** and **CAUTION** statements, and statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.
4. After completing an FRU replacement procedure, extinguish the amber system error light-emitting diode (LED) on the bezel at the top front of the director.

## Using Log Information

The HAFM, Element Manager, and EWS provide access to logs that provide information for administration, operation, and maintenance personnel. Each log stores up to 1,000 entries. The most recent entry displays at the top of a log. If a log is full, a new entry overwrites the oldest entry.

Five logs are accessed through the *HAFM* application:

- **Audit Log**—Displays a history of user actions performed through the *HAFM* application. This information is useful for system administrators and users.
- **Event Log**—Displays events or error conditions recorded by the *HAFM Services* application. Entries reflect the status of the application and managed directors.

Information associated with a call-home failure is intended for use by maintenance personnel to fault isolate the problem, while information provided in all other entries is generally intended for use by third-level support personnel to fault isolate more significant problems.

- **Session Log**—Displays session (login and logout) history for the HAFM appliance, including the date and time, username, and network address of each session. This information is useful for system administrators and users.
- **Product Status Log**—Displays an entry when the status of a director changes. The log reflects the previous status and current status of the director, and indicates the instance of an Element Manager that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification.
- **Fabric Log**—Displays the time and nature of significant changes in the managed fabric.

For a description of the HAFM Logs and an explanation of the button functions at the bottom of the log window, refer to the *hp StorageWorks HA-Fabric Manager User Guide*.

Six logs are accessed through the Element Manager:

- **Director 2/64 Audit Log**—Displays a history of all configuration changes made to a director from the Element Manager, a Simple Network Management Protocol (SNMP) management workstation open systems host, or the maintenance port. This information is useful for administrators and users.

- **Director 2/64 Event Log**—Displays a history of events for the director, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM appliance-to-director communication problems. All detected software and hardware failures are recorded in the Director 2/64 Event Log. The information is useful to maintenance personnel for fault isolation and repair verification.
- **Hardware Log**—Displays a history of FRU removals and replacements (insertions) for the director. The information is useful to maintenance personnel for fault isolation and repair verification.
- **Link Incident Log**—Displays a history of Fibre Channel link incidents (with associated port numbers) for the director. The information is useful to maintenance personnel for isolating port problems (particularly expansion port [E\_Port] segmentation problems) and repair verification.
- **Threshold Alert Log**—Displays details of the threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Configure Threshold Alert(s)** option under the **Configure** menu.
- **Open Trunking Log**—Displays the average data rates of all traffic flows on ISLs (from a receive port to a target domain). Open Trunking also periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimize bandwidth use. The objective of Open Trunking is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

For a description of the Element Manager Logs and an explanation of the button functions at the bottom of the log window, refer to the *hp StorageWorks Director Element Manager User Guide*.

Three logs are accessed through the EWS interface:

- **EWS Event Log**—Displays events or errors recorded at the EWS interface. Entries reflect the status of the interface and managed director. The log stores up to 200 entries, and the most recent entry appears at the top of the log.



- **EWS Open Trunking Re-Route Log**—Displays interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed director.
- **EWS Link Incident Log**—Displays Fibre Channel link incident events recorded at the EWS interface. Entries reflect the cause of the link incident.

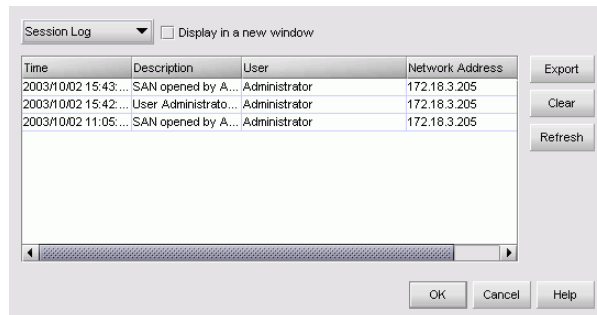
For a description of the EWS Logs and an explanation of the button functions at the bottom of the log window, refer to the *hp StorageWorks Embedded Web Server User Guide*.

## Viewing Logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only login/logout events (session events), open a specific log through the View Logs dialog box.

To view a log, perform the following:

1. Click **Monitor > Logs**, then click one of the options. The View Logs dialog box displays, as shown in [Figure 39](#).



**Figure 39: View Logs dialog box**

- To view a different log, click a log on the drop-down list.
  - To view multiple logs simultaneously, click the **Display in a new window** check box and click another log on the drop-down list.
  - To clear the log, click **Clear**.
  - To refresh the log, click **Refresh**.
  - To export log entries, refer to “[Exporting Log Data](#)” on page 170.
2. Click **OK** to close the dialog box.

## Exporting Log Data

You can export HAFM log data in tab-delimited format. This feature is useful for providing the data to a third-party or including it in a report.

1. Click **Monitor > Logs**, then click one of the options. The View Logs dialog box displays, as shown in [Figure 39](#) on page 169.
2. Click **Export**. The Save dialog box displays.
3. Browse to the folder where you want to save the file. Type a file name in the **File Name** field.
4. Click **Save**. The file is exported in tab-delimited format. To view it in table format, open the file in Microsoft Excel.

## Obtaining Port Diagnostic Information

Port and UPM card diagnostics are performed at the director or HAFM appliance (Element Manager). These diagnostics include:

- Inspecting port and UPM card LEDs at the director.
- Obtaining port degradation or failure information at the Element Manager's Port Card View.
- Obtaining statistical performance information for ports at the Element Manager's **Performance View**.
- Performing internal or external port loopback tests.
- Performing channel wrap tests. The tests apply only to a director configured for FICON management style.
- Inspecting parameters at the EWS interface.

## UPM Card LEDs

To obtain port operational information, inspect port LEDs at the director UPM card faceplate or the emulated port LEDs at the HAFM Hardware View. These port operational states are defined in [Table 22](#).

**Table 22: Port Operational States**

Port State	Green LED	Amber LED	Alert Symbol	Description
Online	On	Off	None	An attached device is connected to the director and ready to communicate, or is communicating with other attached devices. If the port remains online, the green port LED remains illuminated. At the director UPM card, the green LED blinks when there is Fibre Channel traffic through the port.
Offline	Off	Off	None	The director port is blocked and transmitting the offline sequence (OLS) to the attached device.
	Off	Off	Yellow Triangle	The director port is unblocked and receiving the OLS, indicating the attached device is offline.
Beaconing	Off or On	Blinking	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to locate the port.
Invalid Attachment	On	Off	Yellow Triangle	The director port has an invalid attachment state if: (1) a loopback plug is connected to the port with no diagnostic test running, or (2) the port is cabled to another port on the same director, or (3) the port connection conflicts with the configured port type.

**Table 22: Port Operational States (Continued)**

Port State	Green LED	Amber LED	Alert Symbol	Description
Link Incident	Off	Off	Yellow Triangle	A link incident occurred on the port. The alert symbol displays at the Port Card View, Port List View, and Hardware View.
Link Reset	Off	Off	Yellow Triangle	The director and attached device are performing a link reset operation to recover the link connection. This is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is received by the director port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.
Not Operational	Off	Off	Yellow Triangle	The director port is receiving the not operational sequence (NOS) from an attached device.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The director port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented, preventing two connected directors from joining and forming a multi-switch fabric.
Testing	Off	Blinking	Yellow Triangle	The port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	The port is performing an external loopback test.

## HAFM Appliance

To obtain port operational information at the HAFM appliance (Director 2/64 Element Manager), inspect parameters at the:

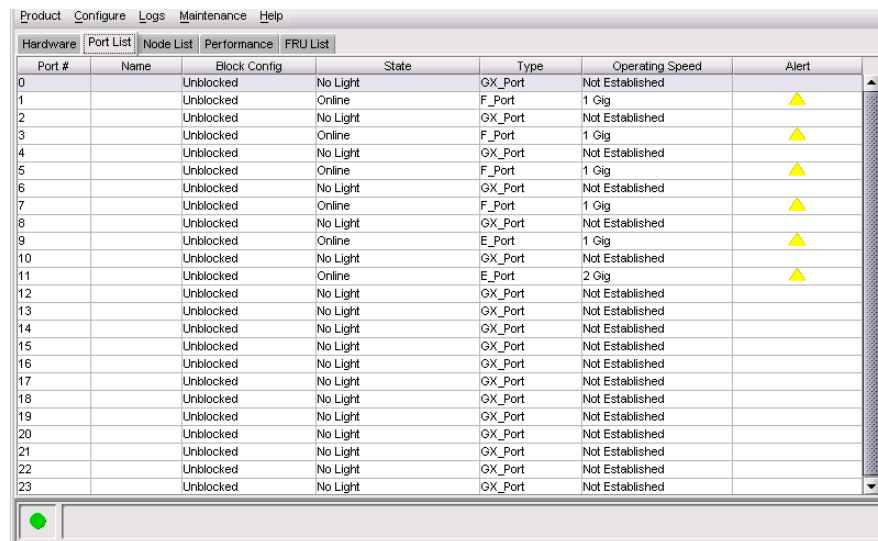
- Port List View
- Performance View
- Port Properties dialog box
- Port Technology dialog box

### Viewing the Port List View

The **Port List View** provides status information for all director ports. The information is useful to maintenance personnel for isolating port problems.

To open the **Port List View**, perform the following:

1. At the Hardware View, click the **Port List** tab. The **Port List View** displays, as shown in [Figure 40](#).



Port #	Name	Block Config	State	Type	Operating Speed	Alert
0		Unlocked	No Light	GX_Port	Not Established	
1		Unlocked	Online	F_Port	1 Gig	▲
2		Unlocked	No Light	GX_Port	Not Established	
3		Unlocked	Online	F_Port	1 Gig	▲
4		Unlocked	No Light	GX_Port	Not Established	
5		Unlocked	Online	F_Port	1 Gig	▲
6		Unlocked	No Light	GX_Port	Not Established	
7		Unlocked	Online	F_Port	1 Gig	▲
8		Unlocked	No Light	GX_Port	Not Established	
9		Unlocked	Online	E_Port	1 Gig	▲
10		Unlocked	No Light	GX_Port	Not Established	
11		Unlocked	Online	E_Port	2 Gig	▲
12		Unlocked	No Light	GX_Port	Not Established	
13		Unlocked	No Light	GX_Port	Not Established	
14		Unlocked	No Light	GX_Port	Not Established	
15		Unlocked	No Light	GX_Port	Not Established	
16		Unlocked	No Light	GX_Port	Not Established	
17		Unlocked	No Light	GX_Port	Not Established	
18		Unlocked	No Light	GX_Port	Not Established	
19		Unlocked	No Light	GX_Port	Not Established	
20		Unlocked	No Light	GX_Port	Not Established	
21		Unlocked	No Light	GX_Port	Not Established	
22		Unlocked	No Light	GX_Port	Not Established	
23		Unlocked	No Light	GX_Port	Not Established	

**Figure 40: Port List View**

The **Port List View** provides status information in the following columns:

- **#**—The director port number (**0** through **63** inclusive).
- **Addr**—The director logical port address (**05** through **43** inclusive) in hexadecimal format (FICON management style only).
- **Name**—The port name configured through the Configure Ports dialog box.
- **Block Config**—The port status (Blocked or Unblocked).
- **State**—The operating state of the port. Valid states are:
  - Online, Offline, or Testing
  - Beaconing
  - Invalid Attachment
  - Link Incident or Link Reset
  - No Light, Not Operational, or Port Failure
  - Segmented E\_Port
- **Type**—The type of port. Valid port types are a generic port (G\_Port) not connected to a Fibre Channel device, director, or switch (therefore light is not transmitted); a fabric port (F\_Port) connected to a device; or an expansion port (E\_Port) connected to a director or switch to form an interswitch link (ISL).
- **Operating Speed**—The operating speed of the port (**Not Established, 1 Gig, or 2 Gig**).
- **Alert**—If Link Incident (LIN) alerts are configured for the port through the Configure Ports dialog box, a yellow triangle displays in the column when a link incident occurs. A yellow triangle also displays if beaconing is enabled for the port. A red and yellow diamond displays if the port fails.

Double-click anywhere in a row for an installed port to open the Port Properties dialog box.

Right-click anywhere in a row for an installed port to open a menu to:

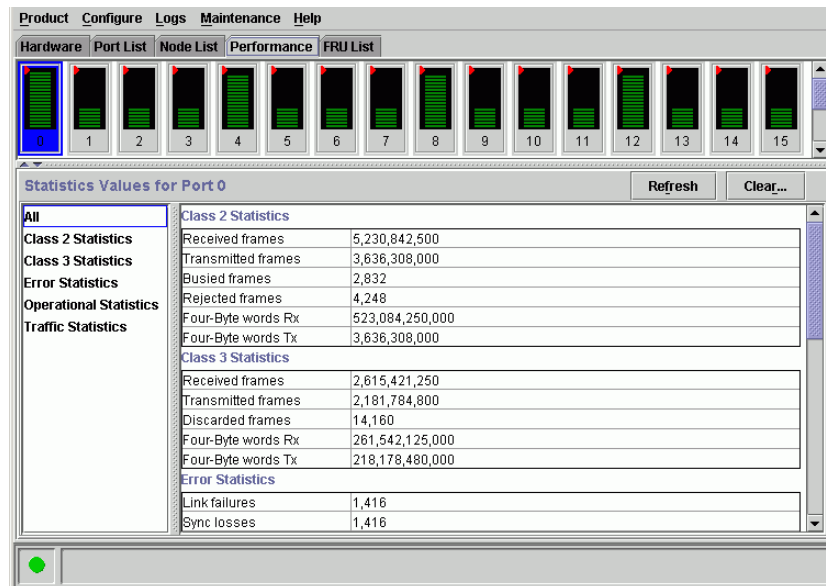
- Open the Port Properties, Node Properties, or Port Technology dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the director is configured for FICON management style.

- Swap one Fibre Channel port address with another. This menu option displays only when the director is configured for FICON management style.
- Clear link incident alerts.
- Reset the port.
- Configure port binding.
- Clear threshold alerts.

## Viewing the Performance View

To view performance data, perform the following:

1. At the Hardware View, click the **Performance** tab. The **Performance View** displays, as shown in [Figure 41](#).



**Figure 41: Performance View**

Each port bar graph in the upper portion of the view displays the instantaneous transmit or receive activity level for the port and is updated every five seconds. The relative value displayed is the greater of either the transmit or receive activity (whichever value is greatest when sampled).

Each port graph has 20 green-bar level indicators corresponding to 5% of the maximum throughput for the port (either transmit or receive). If any activity is detected for a port, at least one green bar appears. A red indicator on each port bar graph (high-water mark) remains at the highest level the graph has reached since the port was set online. The indicator does not display if the port is offline, and it is reset to the bottom of the graph if the port detects a loss of light.

When the mouse cursor is passed over a port bar graph (flyover), the graph highlights with a blue border and an information pop-up displays the port operational state or WWN of the attached device. Click a port bar graph to display statistics values for the port. Right-click a port bar graph to open a pop-up menu to:

- Open the Port Properties, Node Properties, or Port Technology dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping (when the director is configured for FICON management style).
- Swap one Fibre Channel port address with another (when the director is configured for FICON management style).
- Clear link incident alerts.
- Reset the port.
- Enable or disable port binding.
- Clear threshold alerts.

The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Class 2 statistics**—These entries provide information about Class 2 traffic, including:
  - Class 2 frames received and transmitted.
  - Four-byte words received and transmitted.
  - Busied and rejected frames.



- **Class 3 statistics**—These entries provide information about Class 3 traffic, including:
  - Class 3 frames received and transmitted.
  - Four-byte words received and transmitted.
  - Discarded frames.
- **Error statistics**—The **Performance View** displays the following error statistics for the port:
  - **Link failures**—Link failures are recorded in response to an NOS, protocol time-out, or port failure. At the Hardware View, a yellow triangle appears to indicate a link incident, or a blinking red and yellow diamond displays to indicate a port failure.
  - **Sync losses**—Synchronization losses are detected because an attached device was reset or disconnected from the port. At the Hardware View, a yellow triangle displays to indicate a link incident.
  - **Signal losses**—Signal losses are detected because an attached device was reset or disconnected from the port. At the Hardware View, a yellow triangle displays to indicate a link incident.
  - **Primitive sequence errors**—Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations. At the Hardware View, a yellow triangle displays to indicate a link incident.
  - **Discarded frames**—Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the director.
  - **Invalid transmission words**—Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.
  - **CRC errors**—Received frames failed CRC validation, indicating the frames arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
  - **Delimiter errors**—Received frames had frame delimiter errors, indicating the frame arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

- **Address ID errors**—Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.
- **Frames too short**—Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Operational statistics**—These entries provide information about port operation, including:
  - Offline sequences received and transmitted.
  - Link resets received and transmitted.
  - LIPs generated and detected.
- **Traffic statistics**—These entries provide information about port traffic, including:
  - Percent link utilization (receive and transmit).
  - Fibre Channel frames received and transmitted.
  - Four-byte words received and transmitted.
  - Flows rerouted to and from ISLs.

## Viewing Port Properties

To open the Port Properties dialog box, perform the following:

1. Double-click a port in the Port Card View or a port row in the Port List View. The Port Properties dialog box displays, as shown in [Figure 42](#).

Port Number	35
Port Name	
Type	G_Port
Operating Speed	2 Gig
Fibre Channel Address	
Port WWN	
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	No Light
Reason	
Threshold Alert	

**Figure 42: Port Properties dialog box**

The Port Properties dialog box provides the following information:

---

**Note:** If the Open Trunking feature is installed, an additional item, **Congested Threshold %**, displays in the Port Properties dialog box.

---

- **Port Number**—The director port number (**0** through **63** inclusive).
- **Port Name**—The user-defined name or **description** for the port.
- **Type**—The Port type (**G\_Port**, **F\_Port**, or **E\_Port**) type of port (**G\_Port** if nothing is attached to the port, **F\_Port** if a device is attached to the port, and **E\_Port** if the port is connected to another director or switch as part of an ISL).
- **Operating Speed**—The operating speed of the port (**Not Established**, **1 Gbps**, or **2 Gbps**).
- **Fibre Channel Address**—The port's Fibre Channel address identifier.
- **Port WWN**—The Fibre Channel WWN for the director port.
- **Attached Port WWN**—The WWN of the node logged into the port.

- **Block Configuration**—A user-configured state for the port (**Blocked** or **Unblocked**).
- **10-100 km Configuration**—Extended distance buffering. This can be enabled or disabled for the port through the Configure Ports dialog box.
- **LIN Alerts Configuration**—A user-specified state for the port (**On** or **Off**), configured through the Configure Ports dialog box.
- **Beaconing**—User-specified for the port (**On** or **Off**). When beaconing is enabled, a yellow triangle appears adjacent to the status field.
- **Link Incident**—If no link incidents are recorded, **None** appears in the status field. If a link incident is recorded, a summary appears describing the incident, and a yellow triangle appears adjacent to the status field. Valid summaries are:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Link failure - loss of signal or loss of synchronization.
  - Link failure - not-operational primitive sequence received.
  - Link failure - primitive sequence time-out.
  - Link failure - invalid primitive sequence received for the current link state.
- **Operational State**—The state of the port (**Online**, **Offline**, **Beaconing**, **Invalid Attachment**, **Link Incident**, **Link Reset**, **No Light**, **Not Operational**, **Port Failure**, **Segmented E\_Port**, or **Testing**). A yellow triangle appears adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond appears adjacent to the status field if the port fails.
- **Reason**—A summary appears describing the reason if the port state is **Segmented E\_Port**, **Invalid Attachment**, or **Inactive**. For any other port state, the reason field is blank or N/A. Invalid Attachment Messages are explained in [Table 23](#).

**Table 23: Invalid Attachment Messages and Explanations**

Message	Explanation
01 Unknown.	Invalid attachment reason cannot be determined.
02 ISL connection not allowed on this port.	Port is configured as an F_Port, but connected to switch or director.

**Table 23: Invalid Attachment Messages and Explanations (Continued)**

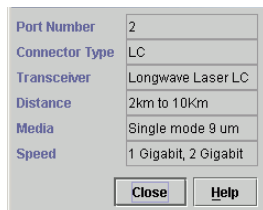
Message	Explanation
03 ELP rejected by the attached switch.	This director or switch transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL (Invalid Attachment only).
04 Incompatible switch at the other end of the ISL.	Interop mode for this switch is set to Open Fabric mode, and the switch at the other end of the ISL is a switch configured for Homogeneous Fabric mode.
05 External loopback adapter connected to the port.	A loopback plug is connected to the port, and there is no diagnostic test running.
06 N_Port connection not allowed on this port.	The port type configuration does not match the actual port use. Port is configured as an E_Port, but it attaches to a node device.
07 Non-homogeneous switch at other end of the ISL.	The cable is connected to a non-homogeneous switch and interop mode is set to homogeneous fabric mode.
08 ISL connection not allowed on this port.	This port type configuration does not match the actual port use (the port is configured as an F_Port, but it attaches to a switch or director).
10 Port binding violation—unauthorized WWN.	The WWN entered to configure port binding is not valid, or a nickname was used that is not configured through the Element Manager for the attached device.
11 Unresponsive node connected to port.	<p>Possible causes are:</p> <ul style="list-style-type: none"> <li>■ Hardware problem on switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login (FLOGI) cannot be received. There may be problems in switch SBAR.</li> <li>■ Faulty or dirty cable connection.</li> <li>■ Faulty host bus adapters that do not send out FLOGI within reasonable time frame.</li> </ul>

- **Threshold Alert**—If a threshold alert exists for the port, an alert indicator (yellow triangle) and the configured name for the alert appear.

## Viewing Port Technology

To open the Port Technology dialog box, perform the following:

1. Right-click a port in the Port Card View or the Port List View. The **Port** menu displays.
2. Click **Port Technology**. The Port Technology dialog box displays, as shown in [Figure 43](#).



**Figure 43: Port Technology dialog box**

The Port Technology dialog box provides the following information:

- **Port Number**—Director port number (**0** through **63** inclusive).
- **Connector type**—Type of port connector (**LC**, **Unknown**, or **Internal Port**).
- **Transceiver**—Type of port transceiver (**Shortwave Laser**, **Longwave Laser**, **Long Distance Laser**, **Unknown**, or **None**).
- **Distance**—Port transmission distance (**50m to 10Km**)
- **Media**—Type of optical cable used (**Singlemode**, **multimode 50-micron**, **multimode 62.5-micron**, or **Unknown**).
- **Speed**—Operating speed (**Not Established**, **1 Gigabit**, or **2 Gigabit**).

## EWS Interface

To obtain port operational information at the EWS interface, inspect parameters at the:

- Monitor Panel—Port List page.
- Monitor Panel—Port Stats page.
- View panel—Port Properties page.

## Viewing the Port List Page

When the EWS interface opens, the **View** panel displays as the default. To view the Port List page, perform the following:

1. At the **View** panel, click **Monitor** on the left side of the panel. The **Monitor** panel displays with the Port List page open, as shown in [Figure 44](#).

Port #	Name	Block Configuration	State	Type
0		Unblocked	Inactive	Gx Port
1		Unblocked	Inactive	Gx Port
2		Unblocked	Inactive	Gx Port
3		Unblocked	Inactive	Gx Port
4		Unblocked	Inactive	Gx Port
5		Unblocked	Inactive	Gx Port
6		Unblocked	Inactive	Gx Port
7		Unblocked	Inactive	Gx Port
8		Unblocked	Inactive	Gx Port
9		Unblocked	Inactive	Gx Port
10		Unblocked	Inactive	Gx Port
11		Unblocked	Inactive	Gx Port

**Figure 44: Monitor panel (Port List page)**

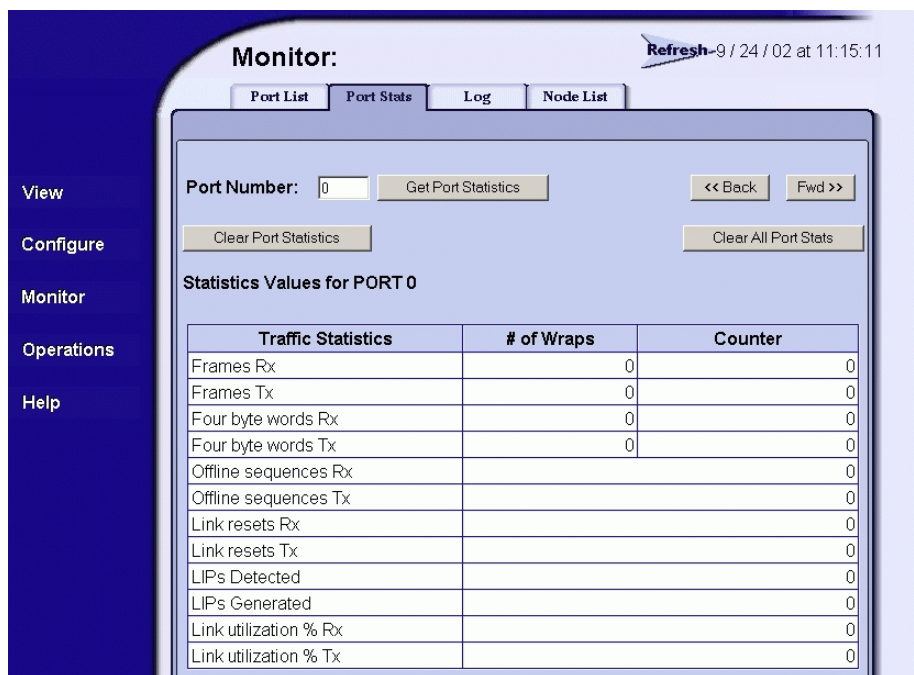
A row of information for each port (**0** through **63** inclusive) appears. Each row consists of the following columns:

- **Port #**—The director port number.
- **Name**—The port name of 24 alphanumeric characters or less. The name typically characterizes the device or fabric element to which the port is attached.
- **Block Configuration**—Indicates if a port is blocked or unblocked. Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the offline sequence (OLS).
- **State**—Port state (**Online**, **Offline**, **Not Installed**, **Inactive**, **Invalid Attachment**, **Link Reset**, **No Light**, **Not Operational**, **Port Failure**, **Segmented E\_Port**, or **Testing**).
- **Type**—The port type (**G\_Port** if nothing is attached to the port, **F\_Port** if a device is attached to the port, and **E\_Port** if the port is connected to another director or switch as part of an ISL).

## Viewing the Port Stats Page

When the EWS interface opens, the **View** panel displays as the default panel. To view the Port Stats page, perform the following:

1. At the **View** panel, click **Monitor** on the left side of the panel. The **Monitor** panel displays with the Port List page open, as shown in [Figure 44](#).
2. Click the **Port Stats** tab. The **Monitor** panel displays with the Port Stats page open, as shown in [Figure 45](#).



**Figure 45: Monitor panel (Port Stats page)**

The Port Stats page displays traffic and error statistics for one port. Values update only when the page opens for a selected port or the user chooses **Get Port Statistics**. The page defaults to port **0**. Increment or decrement the port number displayed (**0** through **63** inclusive) by clicking **Fwd>>** or **<<Back**.



The **# of Wraps** column tracks the number of times the counter wraps for rapidly-growing statistics. The maximum counter value is  $2^{32}$  entries. The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Traffic statistics**—These entries provide information about port traffic, including:
  - Fibre Channel frames received and transmitted.
  - Four-byte words received and transmitted.
  - Offline sequences received and transmitted.
  - Link resets received and transmitted.
  - Loop initialization primitives (LIPs) generated and detected.
  - Percent link utilization (receive and transmit).
- **Error statistics**—The Port Stats page displays the following error statistics for the port:
  - **Link failures**—Link failures are recorded in response to a not operational sequence (NOS), protocol time-out, or port failure.
  - **Sync losses**—Synchronization losses are detected because an attached device was reset or disconnected from the port.
  - **Signal losses**—Signal losses are detected because an attached device was reset or disconnected from the port.
  - **Primitive sequence errors**—Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations.
  - **Discarded frames**—Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the director.
  - **Invalid transmission words**—Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.
  - **CRC errors**—Received frames failed cyclic redundancy check (CRC) validation, indicating the frames arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

- **Delimiter errors**—Received frames had frame delimiter errors, indicating the frame arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber optic cable, or a poor cable connection.
- **Address ID errors**—Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.
- **Frames too short**—Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Class 2 statistics**—These entries provide information about Class 2 traffic, including:
  - Class 2 frames received and transmitted.
  - Four-byte words received and transmitted.
  - Busied and rejected frames.
- **Class 3 statistics**—These entries provide information about Class 3 traffic, including:
  - Class 3 frames received and transmitted.
  - Four-byte words received and transmitted.
  - Discarded frames.

## Viewing the Port Properties Page

When the EWS interface opens, the **View** panel appears as the default panel. To view the Port Properties, perform the following:

1. At the **View** panel, click the **Port Properties** tab. The **View** panel displays with the Port Properties page open, as shown in [Figure 46](#).

<b>View:</b>		Refresh	4 / 12 / 04 at 15:24:58
Director		Port Properties	FRU Properties
Unit Properties		Operating Parameters	Fabric
View	Port Number: 0    Get Port Properties    << Back    Fwd >>		
Configure			
Monitor			
Operations			
Help			
Port Number	0		
Port Name			
Type	E Port		
Operating Speed	1 Gb/sec		
Fibre Channel Address	N/A		
Port WWN	20:04:08:00:88:A0:40:6F		
Attached Port WWN	10:00:08:00:88:A0:54:56		
Block Configuration	Unblocked		
10-100 km Configuration	Off		
Beaconing	Off		
Operational State	Online		
Reason	N/A		
<b>Technology</b>			
Connector Type	LC		
Transceiver	Shortwave Laser		
Distance Capability	Intermediate		
Media	Multi-Mode 50, 62.5 micrometer		
Speed	1 Gb/sec, 2 Gb/sec		

**Figure 46: View panel (Port Properties page)**

The Port Properties page displays information for one port. Values update only when the page opens for a selected port or the user chooses **Get Port Properties**. The page defaults to port **0**. Increment or decrement the port number displayed (**0** through **63** inclusive) by clicking **Fwd>>** or **<<Back**. The page provides the following information:

- **Port Number**—The director port number.
- **Port Name**—The user-defined name or description for the port.

- **Type**—The type of port (**G\_Port** if nothing is attached to the port, **F\_Port** if a device is attached to the port, and **E\_Port** if the port is connected to another director or switch as part of an ISL).
- **Operating Speed**—The operating speed (**Not Established**, **1 Gb/sec**, or **2 Gb/sec**).
- **Fibre Channel Address** — The port's Fibre Channel address identifier.
- **Port WWN**—The Fibre Channel world wide name (WWN) for the port.
- **Attached Port WNN**—The WWN of the node logged into the port.
- **Block Configuration**—The user-configured state for the port (**Blocked** or **Unblocked**).
- **10-100 km Configuration**—Extended distance buffering. This option can be enabled or disabled for the port through the **Configure Ports** dialog box.
- **Beaconing**—The user-specified for the port (**On** or **Off**).
- **Operational State**—The port state (**Online**, **Offline**, **Not Installed**, **Inactive**, **Invalid Attachment**, **Link Reset**, **No Light**, **Not Operational**, **Port Failure**, **Segmented E\_Port**, or **Testing**).
- **Reason**—A summary displays describing the reason if the port state is **Segmented E\_Port**, **Invalid Attachment**, or **Inactive**. For any other port state, the reason is **N/A**.
- **Technology**—Information specific to the installed optical transceiver, including the following: **Connector Type**, **Transceiver**, **Distance Capability**, **Media** (cable type), and **Speed**.

## Performing Loopback Tests

This section describes the procedures to perform an:

- **Internal loopback test**—An internal loopback test checks UPM card circuitry, but does not check fiber optic components of a port transceiver. The test is performed with a device attached to the port, but the test momentarily blocks the port and is disruptive to the attached device.
- **External loopback test**—An external loopback test checks UPM card circuitry, including fiber optic components of a port transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a multi-mode or single-mode loopback plug must be inserted in the port receptacle.

## Internal Loopback Test

To perform an internal loopback test for a single port or a UPM card (four ports):

1. Notify the customer a disruptive internal loopback test will be performed on a port or UPM card. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port or UPM card, and sets attached devices offline.

---

**Note:** At the start of the loopback test, the port or UPM card can be online, offline, blocked, or unblocked.

---

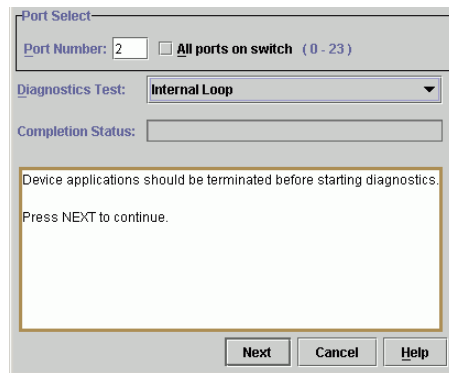
---

**Note:** A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. The device can remain connected during the test.

---

2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The Hardware View for the selected director displays.
4. At the Hardware View, verify the location of the port or UPM card to be tested. When the mouse pointer is passed over a graphical UPM card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:
  - Port card type (UPM).
  - Chassis slot number (**0** through **15** inclusive).
  - The four consecutive port numbers on the selected card. Valid port numbers are in the range of **0** through **63** inclusive.
5. Reset each port to be tested:
  - a. At the Hardware View, double-click the UPM card for which ports are to be tested. The Port Card View displays.
  - b. At the Port Card View, right-click the tested port. A menu displays.
  - c. Click **Reset Port**. A reset warning message box displays.
  - d. Click **OK**. The port resets.
  - e. Click **Back To Full View** to return to the Hardware View.

6. Click **Maintenance > Port Diagnostics**. The Port Diagnostics dialog box displays, as shown in [Figure 47](#).

The image shows a 'Port Select' dialog box. At the top, there is a 'Port Number' field with the value '2' and a checkbox labeled 'All ports on switch (0 - 23)'. Below this is a 'Diagnostics Test' dropdown menu currently set to 'Internal Loop'. Underneath is a 'Completion Status' field. A large text area in the center contains the message: 'Device applications should be terminated before starting diagnostics. Press NEXT to continue.' At the bottom right, there are three buttons: 'Next', 'Cancel', and 'Help'.

**Figure 47: Port Diagnostics dialog box**

7. Select a port or UPM card for test:
  - To select an individual port for test, type the port number (**0** through **63**) in the **Port Number** field.
  - To select a UPM card for test, type the port number of any of the four ports on the card in the **Port Number** field, then click **All ports on card**.
8. Click **Internal Loop** on the **Diagnostics Test** drop-down list.
9. Click **Next**. Beaconing initiates for the port or UPM card selected for test. At the Hardware View, a yellow triangle displays at the top of the UPM card. At the Port Diagnostics dialog box, the message *Verify selected ports are beaconing* displays.
10. Verify beaconing is enabled, then click **Next**. The message *Press START TEST to begin diagnostics* displays, and **Next** changes to **Start Test**.

11. Click **Start Test**. The test begins and:

- **Start Test** changes to **Stop Test**.
- The message Port xx: TEST RUNNING displays, where xx is the port number. If a UPM card is tested, the message displays for all four ports.
- A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

As a port is tested, the amber LED flashes (beacons) and the green LED extinguishes (indicating the port is blocked).

---

**Note:** Click **Stop Test** at any time to abort the loopback test.

---

12. When the test completes, test results display (for each port tested) as Port xx: Passed! or Port xx: Failed! in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.
13. When finished, click **Cancel** to close the Port Diagnostics dialog box and return to the Hardware View. Beaconing is disabled for the port or UPM card.
14. Reset each tested port:
- a. At the Hardware View, double-click the UPM card for which ports were tested. The Port Card View displays.
  - b. At the Port Card View, right-click the tested port. A menu displays.
  - c. Click **Reset Port**. A reset warning box displays.
  - d. Click **OK**. The port resets.

## External Loopback Test

To perform an external loopback test for a single port or a UPM card (four ports):

1. Notify the customer a disruptive external loopback test will be performed on a port or UPM card, and the fiber optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port or UPM card and sets attached devices offline.

---

**Note:** At the start of the loopback test, the port or UPM card can be online, offline, blocked, or unblocked.

---

2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The Hardware View for the selected director displays.
4. At the Hardware View, verify the location of the port or UPM card to be tested. When the mouse pointer is passed over a graphical UPM card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:
  - Port card type (UPM).
  - Chassis slot number (**0** through **15** inclusive).
  - The four consecutive port numbers on the selected card. Valid port numbers are in the range of **0** through **63** inclusive.
5. Reset each port to be tested:
  - a. At the Hardware View, double-click the UPM card for which ports are to be tested. The Port Card View displays.
  - b. At the Port Card View, right-click the tested port. A menu displays.
  - c. Click **Reset Port**. A reset warning box displays.
  - d. Click **OK**. The port resets.
  - e. Click **Back To Full View** to return to the Hardware View.



6. Disconnect the fiber optic jumper cable from the port to be tested. If a UPM card will be tested, disconnect all four fiber optic jumper cables.



**Caution:** If name server zoning is implemented by port number, ensure the fiber optic cables that are disconnected to perform the loopback test are reconnected properly. A cable configuration change disrupts zone operation and may incorrectly include or exclude a device from a zone.

7. If the port to be tested is shortwave laser, insert a multi-mode loopback plug into the port receptacle. If the port to be tested is longwave laser, insert a single-mode loopback plug into the port receptacle. If an entire UPM card will be tested, insert an appropriate loopback plug in all four port receptacles.
8. Click **Maintenance > Port Diagnostics**. The Port Diagnostics dialog box displays, as shown in [Figure 47](#) on page 190.
9. Select a port or UPM card for test:
  - To select an individual port for test, type the port number (**0** through **63**) in the **Port Number** field.
  - To select a UPM card for test, type the port number of any of the four ports on the card in the **Port Number** field, then click **All ports on card**.
10. Click **External Loop** on the **Diagnostics Test** drop-down list.
11. Click **Next**. Beaconing initiates for the port or UPM card selected for test. At the Hardware View, a yellow triangle displays at the top of the UPM card. At the Port Diagnostics dialog box, the message Loopback plugs must be installed on ports being diagnosed displays.
12. Verify loopback plugs are installed and click **Next**. The message Verify selected ports are beaconing displays.
13. Verify that beaconing is enabled and click **Next**. The message Press START TEST to begin diagnostics displays, and **Next** changes to **Start Test**.

14. Click **Start Test**. The test begins and:

- **Start Test** changes to **Stop Test**.
- The message `Port xx: TEST RUNNING` displays, where `xx` is the port number. If a UPM card is tested, the message displays for all four ports.
- A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

As an individual port is tested, the amber LED flashes (beacons) and the green LED illuminates (indicating loopback traffic through the port).

---

**Note:** Click **Stop Test** at any time to abort the loopback test.

---

15. When the test completes, test results display (for each port tested) as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.

16. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the Hardware View. Beaconing is disabled for the port or UPM card.

17. Reset each tested port:

- a. At the Hardware View, double-click the UPM card for which ports were tested. The Port Card View displays.
- b. At the Port Card View, right-click the tested port. A menu displays.
- c. Click **Reset Port**. A reset warning message box displays.
- d. Click **OK**. The port resets.

18. Remove loopback plugs from the tested ports.

19. Reconnect fiber optic jumper cables from devices to tested ports.

## Channel Wrap Test (FICON)

A channel wrap test is a diagnostic procedure that checks FICON host-to-director link connectivity by returning the output of the host as input. The test is host initiated, and transmits **ECHO** extended link service (ELS) command frames to a director port enabled for channel wrapping. The director port echoes the frames back to the host.

To perform a channel wrap test for a director-attached host:

1. Notify the customer a disruptive channel wrap test will be performed on the host-to-director FICON link.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
  - a. Double-click the icon representing the director for which the channel wrap test will be configured. The Hardware View for the selected director displays.
  - b. At the Hardware View, verify the location of the port to be configured for the channel wrap test. When the mouse pointer is passed over a graphical UPM card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:
    - Port card type (UPM).
    - Chassis slot number (**0** through **15** inclusive).
    - The four consecutive port numbers on the selected card. Valid port numbers are in the range of **0** through **63** inclusive.
  - c. Double-click the UPM card with the port to be configured. The Port Card View for the selected card displays.
  - d. Right-click the port to be configured, then click **Channel Wrap**. The Channel Wrap On for Port *n* (where *n* is the port number) window displays.
  - e. Click **OK** to enable channel wrapping for the port.
3. Perform the Fibre Channel link test at the FICON host attached to the configured port. For test instructions, refer to the service documentation delivered with the FICON system.

## Swapping Ports (FICON)

Use the port swap procedure to swap a device connection and logical port address from a failed Fibre Channel port to an operational port. Because both ports are blocked during the procedure, director communication with the attached device is momentarily disrupted.

To perform the port swap procedure for a pair of director ports:

1. Notify the customer a port swap procedure will be performed and a fiber optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The Hardware View for the selected director displays.
4. Click **Maintenance > Swap Ports**. The Swap Ports dialog box displays.
5. Enter the logical port addresses (in hexadecimal format) of the pair of ports to be swapped at the **First address** and **Second address** fields. The ports are automatically blocked during the procedure.
6. Click the **Unblock after swap** check boxes to unblock the ports when the procedure completes.
7. Click **Next**. At the **Swap Ports** dialog box, the message "Continuing this procedure requires varying the selected ports offline. Ask the system operator to vary the link(s) offline, then press Next." displays.
8. Click **Next**. At the Swap Ports dialog box, the message Move the port cable(s). Then press Next. displays.
9. Swap the fiber optic jumper cables between the selected ports, then click **Next**.
10. At the Swap Ports dialog box, the message "Ports swapped successfully." displays. Click **Next** to close the window and return to the Hardware View.

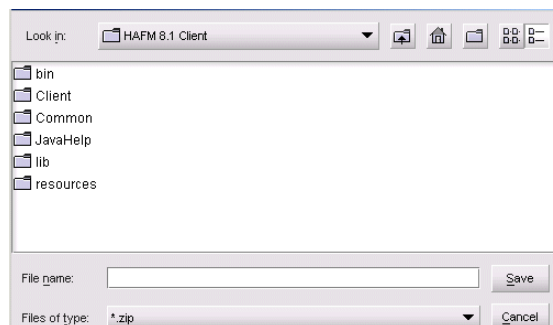
## Collecting Maintenance Data

When the director operational firmware detects a critical error or FRU failure, the director automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the active CTP2 card, then initiates a failover to the operational FRU. The director then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the HAFM appliance hard drive.

**Note:** An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that possibly includes classified Fibre Channel frames) is not included as part of the data collection procedure.

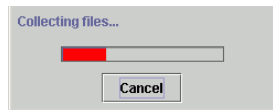
Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by third-level support personnel. Maintenance data includes the dump file, hardware log, audit log, and an engineering log viewable only by support personnel. To collect maintenance data:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director for which the data collection procedure will be performed. The Hardware View for the selected director displays.
3. Click **Maintenance > Data Collection**. The Save Data Collection dialog box displays, as shown in [Figure 48](#).



**Figure 48: Save Data Collection dialog box**

4. Remove the backup CD from the HAFM appliance backup drive and insert a blank backup CD.
5. At the Save Data Collection dialog box, select the backup drive from the **Look in:** drop-down menu, then type a descriptive name for the collected maintenance data in the **File name** field. Ensure the file name has a *.zip* extension, then click **Save**.
6. A dialog box displays, as shown in [Figure 49](#), with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, **Cancel** changes to **Close**.



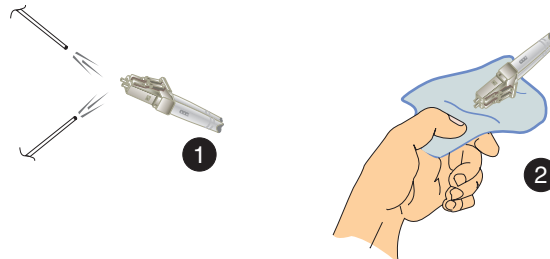
**Figure 49: Data Collection dialog box**

7. Click **Close** to close the dialog box.
8. Remove the backup CD with the newly collected maintenance data from the HAFM appliance backup drive. Return the backup CD with the failed FRU to HP for failure analysis.
9. To ensure the backup application operates normally, replace the original backup CD in the HAFM appliance backup drive.

## Clean Fiber Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber optic cables from director UPM card connectors (if necessary). To clean fiber optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber optic cleaning kit.
2. Disconnect the fiber optic cable from the port. Use compressed air to blow any contaminants from the connector, as shown in ❶ on Figure 50.
  - a. Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
  - b. Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.



**Figure 50: Clean fiber optic components**

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad, as shown in ❷ on Figure 50. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
4. Repeat [step 2](#) and [step 3](#) of this procedure (second cleaning).
5. Repeat [step 2](#) and [step 3](#) of this procedure again (third cleaning), then reconnect the fiber optic cable to the port.

## Power-On Procedure

To power on the director:

1. One alternating current (AC) power cord is required for each power supply installed. Ensure power cords connect facility power to the input power module at the bottom rear of the director. If two power cords are installed for high availability, plug the cords into separate facility power circuits.



**WARNING:** An HP-supplied power cord is provided for each director power supply. To prevent electric shock when connecting the director to primary facility power, use only the supplied power cords, and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

---

2. At the bottom rear of the director, set the power switch (circuit breaker) to the up position. The director powers on and performs power-on self-tests (POSTs). During POSTs:
  - a. Amber LEDs on both CTP2 cards and all UPM cards illuminate momentarily.
  - b. The green LED on each CTP2 card (active and backup) illuminates as the card is tested and UPM cards are tested.
  - c. Green LEDs associated with Fibre Channel ports sequentially illuminate as the ports are tested.
3. After successful POST completion, the green power LED on the front bezel, green LED on the active CTP2 card, and green **PWR OK** LEDs on both power supplies remain illuminated.
4. If a POST error or other malfunction occurs, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.

---

**Note:** When powering on the director after removing and replacing a faulty FRU, the amber system error LED may remain illuminated. Clear the system error LED as part of the replacement procedure.

---



## Power-Off Procedure

Powering the director off and on (performing a power cycle) resets all logic cards and executes POSTs. When performing a power cycle, wait approximately 30 seconds before switching power on.

---

**Note:** When the director is powered off, the operation of attached Fibre Channel devices is disrupted. Do not power off the director unless directed to do so by a procedural step or the next level of support.

---

To power off the director:

1. Notify the customer the director will be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ("[Set Offline State](#)" on page 206).
3. At the bottom rear of the director, set the power switch (circuit breaker) to the down position. The director powers off.
4. If servicing the director, disconnect power cords from the input power module at the bottom rear of the director. This step is not required when performing a power cycle.

## IML, IPL, or Reset the Director

This section describes procedures to IML, IPL, or reset the Director 2/64. An IML or reset is performed at the CTP front panel using the **IML** or the **RESET** button. An IPL is performed from the HAFM appliance (Director 2/64 Element Manager). Do not IPL the director unless directed to do so by a procedural step or the next level of support. An IML and IPL are functionally equivalent. The operations do not cause power-on diagnostics to execute and are not disruptive to Fibre Channel traffic. Both operations:

- Reset the functional logic for the active CTP2 card only. An IPL does not reset the backup CTP2 card, SBAR cards, or UPM cards. All director switching operations continue unaffected.

---

**Note:** An initial machine load (IML) performs essentially the same functions, but resets both CTP2 cards. A director IML is initiated by pressing and holding the white IML button (on the faceplate of either CTP2 card) for three seconds.

---

- Load firmware from the CTP2 card FLASH memory without cycling director power.
- Reset the Ethernet local area network (LAN) interface on the active CTP2 card, causing the connection to the HAFM appliance to drop momentarily until the connection automatically recovers.
- Automatically enable changes to an active zone configuration.
- Keep all fabric logins, name server registrations, and operating parameters intact.
- Automatically set the director online. The blocked or unblocked state of each port remains intact.

## IML the Director from the CTP Front Panel

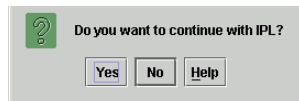
To IML the director from the CTP front panel, perform the following:

1. Press and hold the **IML** button for approximately three seconds.
2. During the IML, the director-to-HAFM appliance Ethernet link drops momentarily and the following occur at the Hardware View:
  - As the network connection drops, the **Director 2/64 Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
  - The status bar at the bottom of the window displays a grey square, indicating director status is unknown.
  - Illustrated FRUs disappear and appear again as the connection is re-established.

## IPL the Director from the HAFM Appliance

To IPL the director from the HAFM appliance, perform the following:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director to be IPLed. The Hardware View for the selected director displays.
3. Click **Maintenance > IPL**. The Information dialog box displays, as shown in [Figure 51](#).



**Figure 51: Information dialog box**

4. Click **Yes** to IPL the director. During the IPL, the director-to-HAFM appliance Ethernet link drops momentarily and the following occur at the Element Manager:
  - As the network connection drops, the **Director 2/64 Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
  - In the HAFM Physical Map, the director icon displays a grey square, indicating director status is unknown.
  - Illustrated FRUs in the Hardware View disappear, and display again as the connection is reestablished.

## Reset the Director from the CTP Front Panel

To reset the director from the CTP front panel, perform the following:

1. Press and hold the **RESET** button for approximately three seconds.
2. During the reset:
  - The green power (**PWR**) LED on the director front panel illuminates.
  - The amber system error (**ERR**) LED on the director front panel blinks momentarily while the director is tested.
  - The green LEDs associated with the Ethernet port blink momentarily while the port is tested.
  - The amber LEDs associated with the ports blink momentarily while the ports are tested.
  - The director-to-HAFM appliance Ethernet link drops momentarily and the following occur at the Hardware View:
    - As the network connection drops, the **Director 2/64 Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
    - In the HAFM Physical Map, the director icon displays a grey square, indicating director status is unknown.
    - Illustrated FRUs in the Hardware View disappear and display again as the connection is reestablished.

## Set the Director Online or Offline

This section describes procedures to set the director online or offline. These operating states are described as follows:

- **Online**—When the director is set online, an attached device can log in to the director if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline**—When the director is set offline, all ports are set offline. The director transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the director.

---

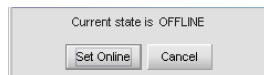
**Note:** When the director is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the director offline unless directed to do so by a procedural step or the next level of support.

---

### Set Online State

To set the director online:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director to be set online. The Hardware View for the selected director displays.
3. Click **Maintenance > Set Online State**. If the director is offline, the Set Online State dialog box displays, as shown in [Figure 52](#), indicating the state is **OFFLINE**.



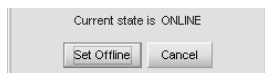
**Figure 52: Set Online State dialog box (offline)**

4. Click **Set Online**. A Warning dialog box displays, indicating the director will be set online.
5. Click **OK**. As the director comes online, observe the Element Manager. The **State** field of the **Director 2/64 Status** table displays **Online**.

## Set Offline State

To set the director offline:

1. Notify the customer the director will be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the director to be set offline. The Hardware View for the selected director displays.
4. Click **Maintenance > Set Online State**. If the director is online, the **Set Online State** dialog box displays, as shown in [Figure 53](#), indicating the state is **ONLINE**.



**Figure 53: Set Online State dialog box (online)**

5. Click **Set Offline**. A Warning dialog box displays, indicating the director will be set offline.
6. Click **OK**. As the director goes offline:
  - The OLS sequence is transmitted to all attached devices.
  - At the Element Manager, the **State** field of the **Director 2/64 Status** table displays **OFFLINE**.

## Block and Unblock Ports

This section describes procedures to block or unblock director ports. An entire UPM card (four ports) can be blocked or unblocked, or ports can be blocked or unblocked on an individual basis. When a port is blocked, the port is automatically set offline. When a port is unblocked, the port is automatically set online.

---

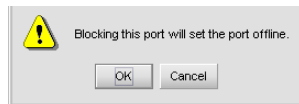
**Note:** When a director port is blocked, the operation of an attached Fibre Channel device is disrupted. Do not block director ports unless directed to do so by a procedural step or the next level of support.

---

### Block a Port

To block an individual director port:

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the director for which a port will be blocked. The Hardware View for the selected director displays.
4. Double-click the UPM card for which a port will be blocked. The Port Card View for the selected card displays.
5. Move the mouse pointer over the port to be blocked and right-click the mouse to open a list of menu options.
6. Click **Block Port**. The Blocking Port warning box displays, as shown in [Figure 54](#).



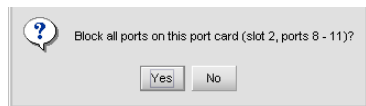
**Figure 54: Blocking Port warning box**

7. Click **OK**. The following occur to indicate the port is blocked (and offline):
  - The emulated green LED associated with the port extinguishes at the Port Card View.
  - The green LED associated with the port extinguishes at the director.
  - A check mark displays in the check box adjacent to the **Block Port** menu option.
8. Click **Back to Full View** to return to the Hardware View.

## Block a UPM Card

To block all four ports on a director UPM card:

1. Notify the customer the UPM card will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the director for which a UPM card will be blocked. The Hardware View for the selected director displays.
4. Double-click the UPM card to be blocked. The Port Card View for the selected card displays.
5. Move the mouse pointer over the UPM card to be blocked (but not over an individual port) and right-click the mouse to open a list of menu options.
6. Click **Block All Ports**. The Block All Ports dialog box displays, as shown in [Figure 55](#).



**Figure 55: Block All Ports dialog box**

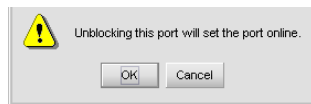
7. Click **Yes**. The following occur to indicate the UPM card is blocked (and offline):
  - Emulated green LEDs associated with all four ports extinguish at the Port Card View.
  - Green LEDs associated with all four ports extinguish at the director.
8. Click **Back to Full View** to return to the Hardware View.



## Unblock a Port

To unblock an individual director port:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director for which a port will be unblocked. The Hardware View for the selected director displays.
3. Double-click the UPM card for which a port will be unblocked. The Port Card View for the selected card displays.
4. Move the mouse pointer over the port to be unblocked and right-click the mouse to open a list of menu options.
5. Click **Block Port**. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. The Unblocking Port warning box displays, as shown in [Figure 56](#).



**Figure 56: Unblocking Port warning box**

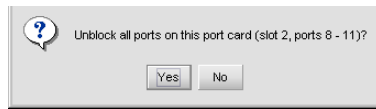
6. Click **OK**. The following occur to indicate the port is unblocked (and online):
  - The emulated green LED associated with the port illuminates at the Port Card View.
  - The green LED associated with the port illuminates at the director.
  - The check box adjacent to the **Block Port** option becomes blank.
7. Click **Back to Full View** to return to the Hardware View.

## Unblock a UPM Card

To unblock all four ports on a director UPM card:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director for which a UPM card will be unblocked. The Hardware View for the selected director displays.
3. Double-click the UPM card to be unblocked. The Port Card View for the selected card displays.
4. Move the mouse pointer over the UPM card to be unblocked (but not over an individual port) and right-click the mouse to open a list of menu options.

5. Click **Unblock All Ports**. The Unblock All Ports dialog box displays, as shown in [Figure 57](#).



**Figure 57: Unblock All Ports dialog box**

6. Click **Yes**. The following occur to indicate the UPM card is unblocked (and online):
  - Emulated green LEDs associated with all four ports illuminate at the Port Card View.
  - Green LEDs associated with all four ports illuminate at the director.
7. Click **Back to Full View** to return to the Hardware View.

## Manage Firmware Versions

Firmware is the director's internal operating code that is downloaded from the HAFM appliance and stored on a CTP2 card. Up to eight versions can be stored on the HAFM appliance hard drive and made available for download to a director. Service personnel can perform the following firmware management tasks:

- Determine the firmware version active on a director.
- Add to and maintain a library of up to 8 firmware versions on the HAFM appliance hard drive.
- Modify a firmware description stored on the HAFM appliance hard drive.
- Delete a firmware version from the HAFM appliance hard drive.
- Concurrently download a firmware version to a selected director.

---

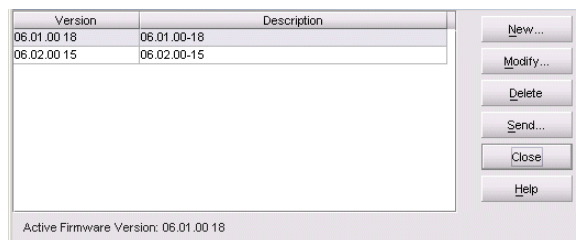
**Note:** The HP StorageWorks HAFM, director, and edge switch release notes include the latest information about supported firmware and HAFM versions.

---

### Determine a Director Firmware Version

To determine a director firmware version:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch to be inspected for firmware version. The Hardware View for the selected switch displays.
3. Click **Maintenance > Firmware Library**. The Director 2/64 Firmware Library dialog box displays, as shown in [Figure 58](#).



**Figure 58: Firmware Library dialog box**

4. The firmware version displays at the lower left corner of the dialog box in **XX.YY.ZZ** format, where **XX** is the version level, **YY** is the release level, and **ZZ** is the patch level.
5. Click **Close** to return to the Hardware View.

## Add a Firmware Version

The firmware version shipped with the director is provided on the *HP StorageWorks Director Documentation Kit CD*. Subsequent firmware versions to upgrade the director are provided to customers through the HP web site.

---

**Note:** When adding a firmware version, follow procedural information in Release Notes that accompany the firmware version. This information supplements information provided in this general procedure.

---

To add a director firmware version to the library stored on the HAFM appliance hard drive:

1. Obtain the new firmware version from the HP web site:

---

**Note:** The following path is subject to change.

---

- a. At the HAFM appliance or other personal computer (PC) with Internet access, open the HP web site. The uniform resource locator (URL) is:  
<http://h18006.www1.hp.com/storage/saninfrastructure.html>

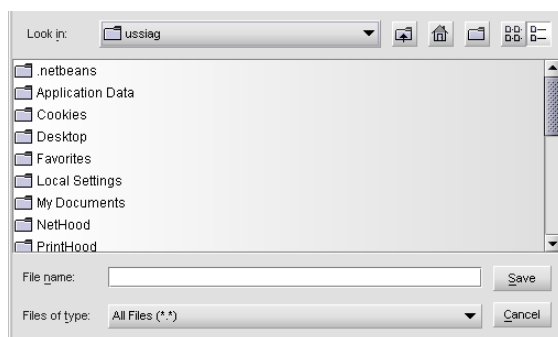
---

**Note:** If required, obtain the customer-specific member name and password from the customer or next level of support.

---

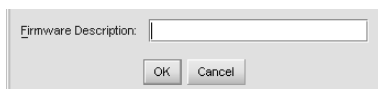
- b. Follow links to HAFM software.
- c. Click the **Director 2/64 Firmware Version XX.YY.ZZ** entry, where **XX.YY.ZZ** is the desired version. The Windows 2000 Save As dialog box displays.

- d. Ensure the correct directory path is specified at the **Save in** field and the correct file is specified in the **File name** field. Click **Save**. The new firmware version is downloaded and saved to the HAFM appliance or PC hard drive.
  - e. If the new firmware version was downloaded to a PC (not the HAFM appliance), transfer the firmware version file to the HAFM appliance by backup disk, CD-ROM, or other electronic means.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
  3. Double-click the icon representing the director to which the firmware version will be added. The Hardware View for the selected director displays.
  4. Click **Maintenance > Firmware Library**. The Director 2/64 Firmware Library dialog box displays, as shown in [Figure 58](#) on page 211.
  5. Click **New**. The New Firmware Version dialog box displays, as shown in [Figure 59](#).



**Figure 59: New Firmware Version dialog box**

6. Select the desired firmware version file (downloaded in [step 1](#)) from the HAFM appliance CD-ROM or hard drive. Ensure the correct directory path and filename display in the **File name** field and click **Save**. The New Firmware Description dialog box displays, as shown in [Figure 60](#).



**Figure 60: New Firmware Description dialog box**

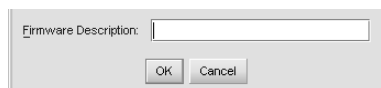
7. Enter a description (up to 24 characters in length) for the new firmware version and click **OK**. It is recommended the description include the installation date and text that uniquely identifies the firmware version.

8. A **Transfer Complete** message box displays, indicating the new firmware version is stored on the HAFM appliance hard drive. Click **Close** to close the message box.
9. The new firmware version and associated description display in the Director 2/64 Firmware Library dialog box.
10. Click **Close**.
11. To send the firmware version to a director, see “[Download a Firmware Version to a Director](#)” on page 215.

## Modify a Firmware Version Description

To modify the description of a director firmware version in the library stored on the HAFM appliance hard drive:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director for which the firmware version description will be modified. The Hardware View for the selected director displays.
3. Click **Maintenance > Firmware Library**. The Director 2/64 Firmware Library dialog box displays, as shown in [Figure 58](#) on page 211.
4. Select the firmware version to be modified and click **Modify**. The Modify Firmware Description dialog box displays, as shown in [Figure 61](#).



**Figure 61: Modify Firmware Description dialog box**

5. Enter a modified description (up to 24 characters) for the firmware version and click **OK**. It is recommended the description include the installation date and text that uniquely identifies the firmware version.
6. The new description for the firmware version displays in the Director 2/64 Firmware Library dialog box.
7. Click **Close**.

## Delete a Firmware Version

To delete a director firmware version from the library stored on the HAFM appliance hard drive:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director from which the firmware version will be deleted. The Hardware View for the selected director displays.
3. Click **Maintenance > Firmware Library**. The Director 2/64 Firmware Library dialog box displays, as shown in [Figure 58](#) on page 211.
4. Select the firmware version to be deleted and click **Delete**. A confirmation dialog box displays.
5. Click **OK**. The selected firmware version is deleted from the Director 2/64 Firmware Library dialog box.
6. Click **Close**.

## Download a Firmware Version to a Director

This procedure downloads a selected firmware version from the HAFM appliance library to a director managed by the open instance of the Element Manager. The procedure applies to a director with two (redundant) CTP2 cards. The process occurs concurrently without taking the director offline or disrupting operation. The new firmware version takes effect when control is passed from the active to the backup CTP2 card. Although director operation is not affected, name server, alias server, and login server functions are momentarily unavailable during CTP2 card switchover.

---

**Note:** When downloading a firmware version, follow procedural information in release notes that accompany the firmware version. This information supplements information provided in this general procedure.

---

To download a firmware version to a director:

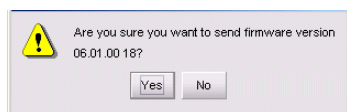
1. Open the *HAFM* application. The View All - HAFM 8 main window displays.

2. Before downloading firmware version **XX.YY.ZZ** to a director, ensure that the required version of the *HAFM* application, as described in the firmware release notes, is running on the HAFM appliance.
  - a. Click **Help > About**. The About dialog box displays and lists the *HAFM* application version. Click **OK** to close the dialog box.
  - b. If required, install the correct version of the *HAFM* application (“[Install or Upgrade Software](#)” on page 223).
3. Double-click the icon representing the director to which the firmware version will be downloaded. The Hardware View for the selected director displays.
4. As a precaution to preserve director configuration information, perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
5. Click **Maintenance > Firmware Library**. The Director 2/64 Firmware Library dialog box displays, as shown in [Figure 58](#) on page 211.
6. Select the firmware version to be downloaded and click **Send**. The send function verifies existence of certain director conditions before the download process begins.

If an error occurs, a message displays, indicating the problem must be fixed before firmware is downloaded. Conditions that terminate the process include:

- A redundant CTP2 card failure.
- The firmware version is being installed to the director by another user.
- The director-to-HAFM appliance link is down.

If a problem occurs and a corresponding message displays, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem. If no error occurs, the Send Firmware confirmation box displays, as shown in [Figure 62](#).



**Figure 62: Send Firmware dialog box**



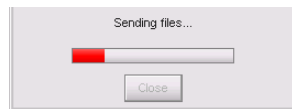
7. Click **Yes**. The **Send Firmware** dialog box displays.

As the download begins, a `Writing data to FLASH` message displays at the top of the dialog box, followed by a `Sending Files` message. This message remains as a progress bar travels across the dialog box to show percent completion of the download. The bar progresses to 50% when the last file is transmitted to the first CTP2 card. The bar remains at the 50% point until the director performs an IPL (indicated by an `IPLing` message).

During the IPL, the director-to-HAFM appliance link drops momentarily and the following occur at the Element Manager:

- As the network connection drops, the Director 2/64 Status table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
- In the HAFM Physical Map, the director icon displays a grey square, indicating director status is unknown.
- Illustrated FRUs in the Hardware View disappear and display again as the connection is reestablished.

After the IPL, a `Synchronizing CTPs` message displays. This message remains as files are transmitted to the second CTP2 card and the progress bar travels across the dialog box to 100%. When the download reaches 100%, a `Send Firmware Complete` message displays, as shown in [Figure 63](#).



**Figure 63: Send Firmware Complete dialog box**

8. Click **Close** to close the dialog box.
9. Click **Close**.

## Manage Configuration Data

The Element Manager provides maintenance options to back up, restore, or reset the configuration files stored in nonvolatile random-access memory (NV-RAM) on both director CTP2 cards. Configuration data in the file includes:

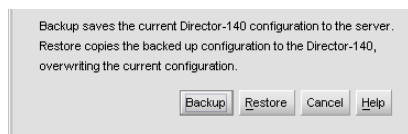
- Identification data (director name, description, and location).
- Port configuration data (port names, blocked states, extended distance settings).
- Operating parameters (buffer-to-buffer credit [BB\_Credit] value, error-detect time-out value [E\_D\_TOV], resource allocation time-out value [R\_A\_TOV], switch priority, and preferred domain ID).
- SNMP configuration information, including trap recipients, community names, and write authorizations.
- Zoning configuration information, including the active zone set and default zone state.

The backup file is not required in a redundant director. However, the feature is available and may be useful to save a special-purpose configuration for test. The director must be set offline prior to restoring or resetting the configuration file.

## Back up the Configuration

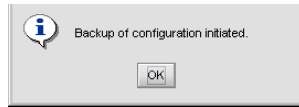
To back up the director configuration file to the HAFM appliance:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the director for which the configuration file will be backed up. The Hardware View for the selected director displays.
3. Click **Maintenance > Backup & Restore Configuration**. The Backup and Restore Configuration dialog box displays, as shown in [Figure 64](#).



**Figure 64: Backup and Restore Configuration dialog box**

4. Click **Backup**. When the backup process finishes, the Backup Complete dialog box displays, as shown in [Figure 65](#).



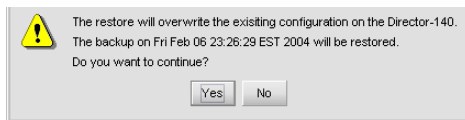
**Figure 65: Backup Complete dialog box**

5. Click **OK** to close the dialog box and return to the Hardware View.

## Restore the Configuration

To restore the director configuration file from the HAFM appliance:

1. Notify the customer the director will be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ("[Set Offline State](#)" on page 206).
3. Open the *HAFM* application. The View All - HAFM 8 main window displays.
4. Double-click the icon representing the director for which the configuration file will be restored. The Hardware View for the selected director displays.
5. Click **Maintenance > Backup & Restore Configuration**. The Backup and Restore Configuration dialog box displays, as shown in [Figure 64](#) on page 218.
6. Click **Restore**. A Warning message box displays, as shown in [Figure 66](#).



**Figure 66: Warning dialog box**

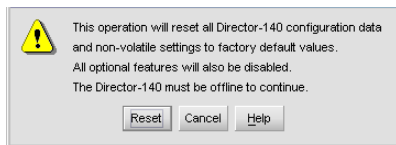
7. Click **Yes**. When the restore process finishes, the Restore Complete dialog box displays.
8. Click **OK** to close the dialog box and return to the Hardware View.

## Reset Configuration Data

**Note:** This procedure resets the director IP address to the default value of **10.1.1.10** and may disrupt HAFM appliance-to-director communication. All configured feature (PFE) keys must be re-entered.

To reset director data to the factory default settings:

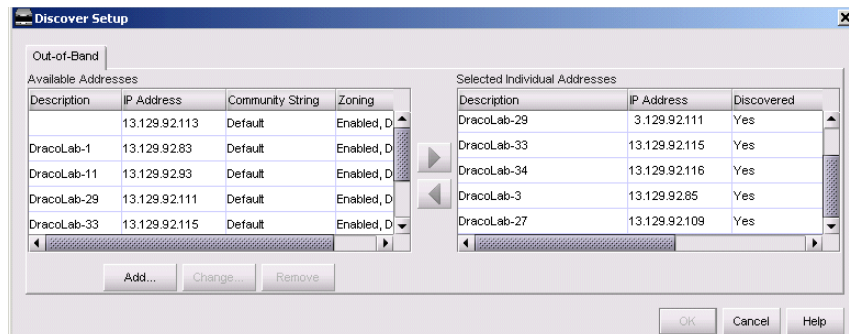
1. Notify the customer the director will be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ("[Set Offline State](#)" on page 206).
3. Open the *HAFM* application. The View All - HAFM 8 main window displays.
4. Double-click the icon representing the director for which the configuration file will be reset to factory default settings. The Hardware View for the selected director displays.
5. Click **Maintenance > Reset Configuration**. The Reset Configuration dialog box displays, as shown in [Figure 67](#).



**Figure 67: Reset Configuration dialog box**

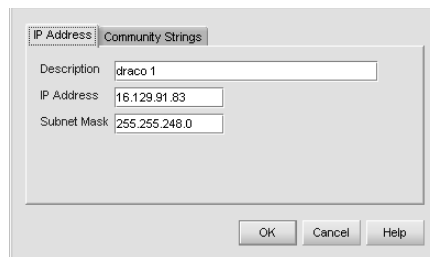
6. Click **Reset**. When the process completes, the dialog box closes and the application returns to the Hardware View.
7. The director IP address resets to the default address of **10.1.1.10**.
  - If the configured IP address (prior to reset) was the same as the default address, the director-to-HAFM appliance Ethernet link is not affected and the procedure is complete.
  - If the configured IP address (prior to reset) was not the same as the default address, the director-to-HAFM appliance Ethernet link drops and HAFM appliance communication is lost. Continue to the next step.
8. To change the director IP address and restart the HAFM appliance session, go to [step 10](#).

9. To restart a HAFM appliance session using the default IP address of **10.1.1.10**:
  - a. Close the Director 2/64 Element Manager and return to the *HAFM* application.  
A grey square with a yellow exclamation mark displays adjacent to the icon representing the reset director, indicating the director is not communicating with the HAFM appliance.
  - b. At the *HAFM* application, click **Discover > Setup**. The Discover Setup dialog box displays, as shown in [Figure 68](#).



**Figure 68: Discover Setup dialog box**

- c. Highlight the entry representing the director in the Available Addresses window and click **Change**. The Domain Information dialog box displays, as shown in [Figure 69](#).



**Figure 69: Domain Information dialog box**

- d. Enter 10.1.1.10 in the **IP Address** field and click **OK**. Entries at the Discover Setup dialog box reflect the new IP address.
  - e. At the Discover Setup dialog box, click **OK**. Director-to-HAFM appliance communication is restored and the procedure is complete.

10. Change the director IP address and restart the HAFM appliance session as follows:
  - a. A grey square with a yellow exclamation mark displays adjacent to the icon representing the reset director, indicating director is not communicating with the HAFM appliance.
  - b. Delete the icon representing the reset director. At the *HAFM* application, click **Discover > Setup**. The Discover Setup dialog box displays, as shown in [Figure 68](#) on page 221.
  - c. Highlight the entry representing the reset director in the Available Addresses window and click **Remove**.
  - d. At the Discover Setup dialog box, click **OK**. The director is no longer defined to the HAFM appliance.
  - e. Change a director IP address through the maintenance port. Refer to *hp StorageWorks Director 2/64 Installation Guide* for more information.
  - f. Identify the switch to the *HAFM* application. Refer to *hp StorageWorks Director 2/64 Installation Guide* for more information.
  - g. Director-to-HAFM appliance communication is restored and the procedure is complete.

## Install or Upgrade Software

This section describes the procedure to install or upgrade the *HAFM* application to the HAFM appliance. The *HAFM* application includes the *Director 2/64 Element Manager* and *HAFM Services* applications.

The *HAFM* application shipped with the director is provided on the *HAFM* Applications CD-ROM. Subsequent software versions for upgrading the director are provided to customers through the *HAFM* application's CD-ROM or through the HP web site.

---

**Note:** When installing or upgrading a software version, follow all procedural information in Release Notes that accompany the software version. This information supplements information provided in this general procedure.

---

To install or upgrade the *HAFM* application and associated applications to the HAFM appliance:

1. Log out of all *HAFM* application sessions (local and remote).
2. Obtain the new software version from the HP web site:

---

**Note:** The following path is subject to change.

---

- a. At the HAFM appliance or other personal computer (PC) with Internet access, open the HP web site. The uniform resource locator (URL) is:  
<http://h18006.www1.hp.com/storage/saninfrastructure.html>

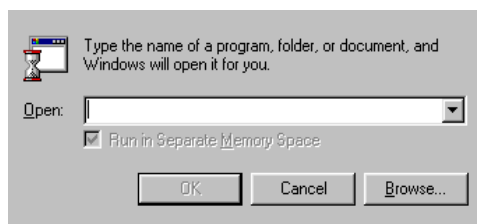
---

**Note:** If required, obtain the customer-specific member name and password from the customer or next level of support.

---

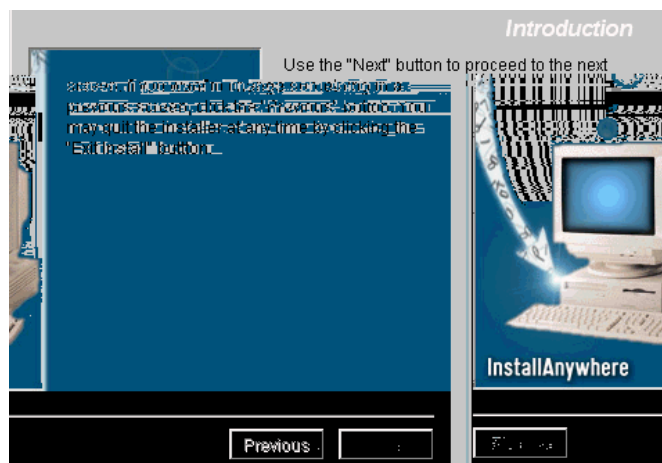
- b. Follow links to HAFM software.
- c. Click the **HAFM Software Version XX.YY.ZZ** entry, where **XX.YY.ZZ** is the desired version. The Windows 2000 Save As dialog box displays.

- d. Ensure the correct directory path is specified at the **Save in** field and the correct file is specified in the **File name** field. Click **Save**. The new HAFM version is downloaded and saved to the HAFM appliance or PC hard drive.
  - e. If the new HAFM version was downloaded to a PC (not the HAFM appliance), transfer the HAFM software version file to the HAFM appliance by CD-ROM or other electronic means.
3. Click **Start > Run**. The Run dialog box displays, as shown in [Figure 70](#).



**Figure 70: Run dialog box**

4. At the Run dialog box, select the directory path (hard drive or CD-ROM drive) and filename of the executable file (*HAFM\_SERVERINSTALL.EXE*) using **Browse**. The directory path and filename display in the **Open** field.
5. Click **OK**. A series of message boxes displays as the *InstallAnywhere* application, as shown in [Figure 71](#), prepares to install the *HAFM* application software, followed by the HP StorageWorks HA-Fabric Manager dialog box.



**Figure 71: InstallAnywhere dialog box (Introduction)**



6. Follow the online instructions for the *InstallAnywhere* program. Click **Next**, **Install**, or **Done** as appropriate.
7. Power off and reboot the HAFM appliance.
  - a. Simultaneously press **Ctrl + Alt + Delete** to display the Windows 2000 Logon Information dialog box.
  - b. Type the username and password and click **OK**. The Windows 2000 desktop displays.

---

**Note:** If required, obtain the username and password from the customer or next level of support.

---

8. The *HAFM* application automatically opens and the HAFM 8 Log In dialog box displays, as shown in [Figure 9](#) on page 49.
9. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the network address is *localhost*.  
The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.  
If you want to connect to a HAFM appliance that is not listed, enter the IP address in the **Network Address** field.
10. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.
11. If you want your computer to save the login information, click **Save Password**.
12. Click **Login**. The View All - HAFM 8 window displays, as shown in [Figure 10](#) on page 50.

---

**Note:** If required, obtain the username, password, and HAFM appliance name from the customer or next level of support.

---



# FRU Removal and Replacement

## 4

This chapter describes removal and replacement procedures (RRPs) used by authorized service representatives for all director field-replaceable units (FRUs). Do not perform a procedure in this chapter until a failure is isolated to an FRU. If fault isolation was not performed, go to “[MAP 0000: Start MAP](#)” on page 46. This chapter includes:

- [Factory Defaults](#), page 228
- [Procedural Notes](#), page 228
- [Remove and Replace FRUs](#), page 229

## Factory Defaults

Table 24 lists the defaults for the passwords and IP, subnet, and gateway addresses.

**Table 24: Factory-set Defaults**

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Procedural Notes

---

**Note:** HAFM and Element Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed, and the fields may contain data that does not match the data seen on your system.

---

The following procedural notes are referenced as applicable. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing an FRU repair, read the removal and replacement procedures for that FRU carefully and thoroughly to familiarize yourself with the procedures, and to reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all electrostatic discharge (ESD) procedures, **WARNING** and **CAUTION** statements, and statements listed in the preface of this manual.
3. After completing the steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.
4. After completing a replacement procedure, clear the event code reporting the failure and the event code reporting the recovery from the Director 2/64 Event Log (at the HAFM appliance), and extinguish the amber system error light-emitting diode (LED) at the director front bezel.

## Remove and Replace FRUs

This section describes procedures to remove and replace director FRUs, along with a list of tools required to perform each procedure. In addition, the section provides:

- ESD information.
- A list of concurrent FRUs. Concurrent FRUs can be removed and replaced while the director is powered on and operational.
- A list of non-concurrent FRUs. Non-concurrent FRUs can only be removed and replaced after the director is powered off.

See “[Illustrated Parts Breakdown](#)” on page 265 for FRU locations and part numbers.

### ESD Information

When performing procedures described in this section, follow all ESD procedures, **WARNING** statements, and **CAUTION** statements.



**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

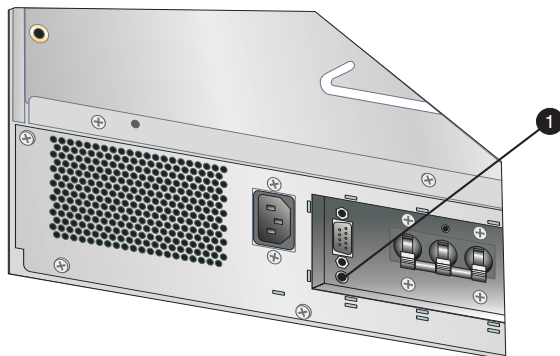
The ESD grounding point for the front of the chassis (❶) is located at the bottom center, adjacent to the left power supply, as shown in [Figure 72](#). Touch the chassis once before performing any maintenance action, and once each minute while removing or replacing FRUs.

If the director is not connected to facility power (and therefore not grounded), connect the ESD wrist strap to an approved bench grounding point instead of the chassis.



**Figure 72: ESD grounding point (front)**

The ESD grounding point for the rear of the chassis (❶) is located at the bottom center, directly below the maintenance port, as shown in [Figure 73](#). Touch the chassis once before performing any maintenance action, and once each minute while removing or replacing FRUs.



**Figure 73: ESD grounding point (rear)**

## Concurrent FRUs

[Table 25](#) lists concurrent FRUs. Concurrent FRUs can be removed and replaced while the director is powered on and operational. The table also lists ESD precaution requirements (yes or no) for each FRU and provides hyperlinks to the removal and replacement procedure.

**Table 25: Concurrent FRU Names and ESD Requirements**

Concurrent FRU Name	ESD Precaution Requirement
Control processor card (" <a href="#">RRP: Redundant CTP2 Card</a> " on page 231)	Yes
Universal port module card (" <a href="#">RRP: UPM Card</a> " on page 236)	Yes
Small form factor pluggable (SFP) optical transceiver (" <a href="#">RRP: SFP Optical Transceiver</a> " on page 241)	No
UPM filler blank (" <a href="#">RRP: UPM Filler Blank</a> " on page 244)	No

**Table 25: Concurrent FRU Names and ESD Requirements (Continued)**

Concurrent FRU Name	ESD Precaution Requirement
Power supply ("RRP: Redundant Power Supply" on page 245)	Yes
Serial crossbar assembly ("RRP: Redundant SBAR Assembly" on page 248)	Yes
Fan module ("RRP: Redundant Fan Module" on page 252)	Yes

## Non-Concurrent FRUs

Table 26 lists non-concurrent FRUs. Non-concurrent FRUs are removed and replaced after the director is powered off. The table also lists ESD precaution requirements (yes or no) for each FRU, and references the page number of the removal and replacement procedure.

**Table 26: Non-Concurrent FRU Names and ESD Precautions**

Non-Concurrent FRU Name	ESD Precaution Requirement
Power module assembly ("RRP: Power Module Assembly" on page 255)	Yes
Backplane ("RRP: Backplane" on page 258)	Yes

## RRP: Redundant CTP2 Card

Use the following procedures to remove or replace a redundant CTP2 card (two cards in the director) with the backup CTP2 card operational. A list of tools required is provided.



**Caution:** Do not remove and replace a redundant CTP2 card if the backup CTP2 card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

## Tools Required

The following tools are required to perform these procedures.

- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).

## Removing a Redundant CTP2 Card

To remove a redundant CTP2 card:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the customer representative.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 72](#).



**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

3. Identify the defective CTP2 card from the amber LED on the card or failure information at the Hardware View.
4. Disconnect the Ethernet local area network (LAN) cable from the RJ-45 connector on the card faceplate.
5. The CTP2 card is secured to the director chassis with two captive Allen screws. The bottom screw is spring-loaded and locks the CTP2 card in place. The top screw cams the CTP2 card into and out of the backplane.



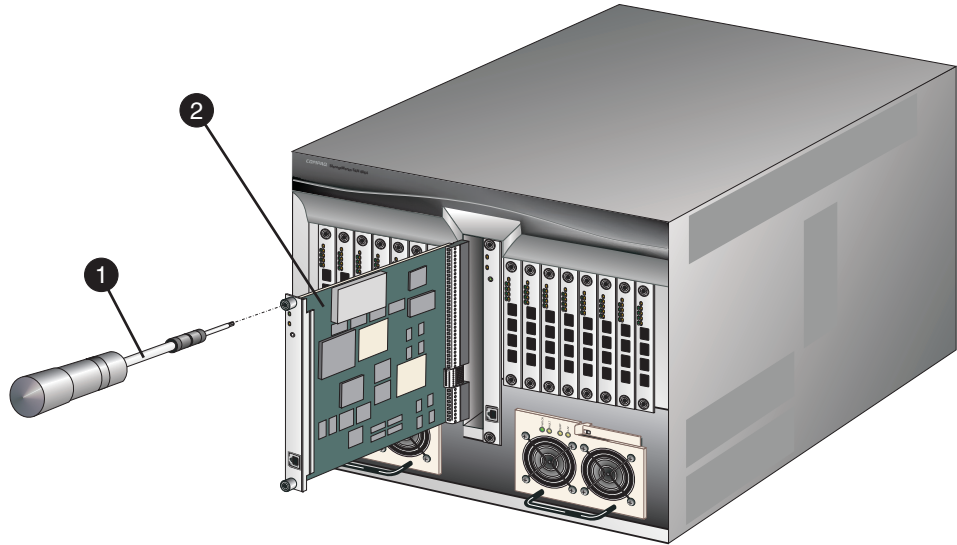
**Caution:** The torque tool supplied with the director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

---

- a. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the screw counterclockwise until the spring releases and the tool turns freely.



- b. Insert the torque tool(❶) into the cam Allen screw at the top of the card(❷). To unseat the CTP2 card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely, as shown in [Figure 74](#).



SHR-2286

**Figure 74: CTP2 card removal and replacement**

6. Pull the CTP2 card from its card track and remove it from the director chassis. Place the card in an antistatic bag to provide ESD protection.

## Replacing a Redundant CTP2 card

To replace a redundant CTP2 card:

1. Wait approximately 20 seconds after removal of the failed CTP2 card to begin this replacement procedure.
2. Remove the replacement card from its protective antistatic bag.
3. Hold the card by its stiffener and insert it in the chassis card track, as shown in [Figure 74](#). The label identifying the card should be at the top. Verify the card is aligned in the card tracks, then slide it forward until it makes contact with the backplane.

4. Secure the CTP2 card:
  - a. Insert the torque tool into the cam Allen screw at the top of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.
  - b. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.
  - c. Verify the card stiffener is flush with the front of the card cage and even with other director logic cards.
5. After the replacement CTP2 card is installed, note the following:
  - When a CTP2 card with a different firmware version is installed in a director with an active CTP2 card, a synchronization process occurs. This process causes firmware from the active CTP2 card to be downloaded to the replacement CTP2 card. The process does not occur if both CTP2 cards have the same firmware version.
  - The synchronization process may take up to ten minutes (depending on director activity).



**Caution:** Allow the synchronization process to complete. If the process is interrupted by a director power cycle or initial program load (IPL), or by removing the replacement CTP2 card, the card may be unusable due to partially-loaded firmware.

---

- If after ten minutes the replacement CTP2 card is not operational, perform the data collection procedure ("[Collecting Maintenance Data](#)" on page 197) and return the failed replacement card to HP.
  - Do not reinstall the failed replacement CTP2 card, because this can corrupt director firmware. Obtain a new CTP2 card and perform this replacement procedure.
6. Verify that synchronization is complete by viewing the **Event Log**.
  7. Connect the Ethernet LAN cable to the RJ-45 connector on the faceplate of the replacement CTP2 card.
  8. Disconnect the ESD wrist strap from the director chassis and your wrist.

9. Inspect the CTP2 card to ensure the amber LED is extinguished. If the amber LED is illuminated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
10. At the Hardware View, click **Logs > Event Log**. The Event Log displays. Ensure the following event codes display in the log:
  - **410**—CTP2 card reset.
  - **416**—Backup CTP2 installed.
  - **422**—CTP2 firmware synchronization complete (only if the firmware versions on the two CTP2 cards are different).If the event codes do not display in the log, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
11. Perform one of the following to verify CTP2 card operation:
  - At the Hardware View, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
  - At the EWS interface, open the **Switch** tab at the View panel and ensure no amber LEDs illuminate that indicate a CTP2 card failure. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
12. At the Hardware View, double-click the graphic representing the replacement card to open the FRU Properties dialog box. Verify that CTP2 card information (FRU name, position, and state) is correct. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
13. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
14. If the customer requests the replacement CTP2 card be set as the active card, perform an FRU switchover. At the Hardware View, right-click the graphic representing the replacement card to open a menu, then click **Switchover**.
15. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.

- If at an EWS interface:
  - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
  - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
  - c. Click **Clear Light**.

16. If necessary, close and lock the equipment cabinet door.

## RRP: UPM Card

Use the following procedures to remove or replace a UPM card. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).
- Fiber optic protective plugs (provided with the director).
- Protective caps (provided with fiber optic jumper cables).
- Fiber optic cleaning kit.

### Removing a UPM Card

To remove a UPM card:

1. Notify the customer that all ports on the defective UPM card will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through any operational ports on the card and sets attached devices offline.
2. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the customer representative.

3. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 72](#) on page 229.



**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

4. Identify the defective UPM card from the amber LED on the card or failure information at the Hardware View.
5. Block communication to the defective UPM card (“[Block a UPM Card](#)” on page 208).
6. Disconnect the fiber optic jumper cable from each port on the defective card. Repeat this step for all four ports.
  - a. Pull the keyed LC connector free from the port’s optical transceiver.
  - b. Place a protective cap over the cable connector. If required, label jumper cables to ensure correct connections when the UPM card is replaced.

---

**Note:** If name server zoning is implemented by port number, a change to the director fiber optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

---

- c. Insert a protective plug into the optical transceiver.



**WARNING:** When fiber optic cables are disconnected from UPM card optical transceivers, ensure protective plugs are inserted into the receptacles. This prevents damage to sensitive components and prevents injury to the eye if the laser is viewed directly.

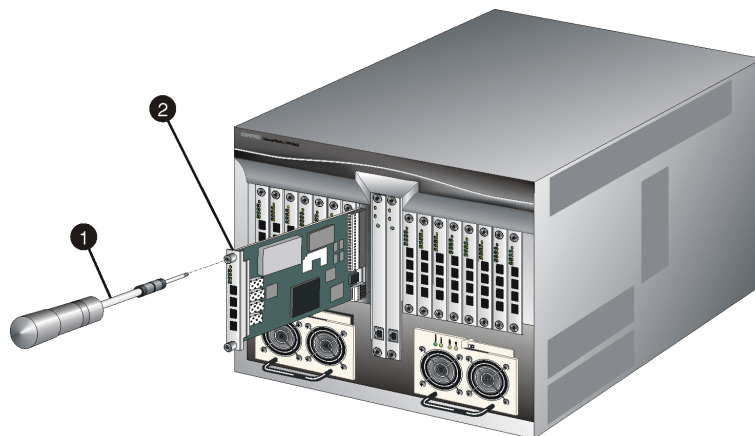
---

7. The UPM card is secured to the director chassis with two captive Allen screws. The bottom screw is spring-loaded and locks the UPM card in place. The top screw cams the UPM card into and out of the backplane.



**Caution:** The torque tool supplied with the Director 2/64 is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

- a. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the screw counterclockwise until the spring releases and the tool turns freely.
  - b. Insert the torque tool(❶) into the cam Allen screw at the top of the card (❷). To unseat the UPM card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely, as shown in [Figure 75](#).
8. Pull the UPM card from its card track and remove it from the director chassis. Place the card in an antistatic bag to provide ESD protection.



SHR-2302

**Figure 75: UPM card removal and replacement**

## Replacing a UPM Card

To replace a UPM card:

1. Remove the replacement card from its protective antistatic bag.
2. Hold the card by its stiffener and insert it in the chassis card track, as shown in [Figure 75](#) on page 238. The label identifying the card should be at the top. Verify the card is aligned in the card tracks, then slide it forward until it makes contact with the backplane.
3. Secure the UPM card:
  - a. Insert the torque tool into the cam Allen screw at the top of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.
  - b. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.
  - c. Verify the card stiffener is flush with the front of the card cage and even with other director logic cards.
4. Perform an external loopback test for all ports on the replacement UPM card (“[External Loopback Test](#)” on page 192). If the test fails, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
5. Reconnect a fiber optic jumper cable to each port on the card. Inspect the label on the jumper cable to ensure the correct connection. Repeat this step for all four ports.
  - a. Remove the protective cap from the cable connector and the protective plug from the port’s optical transceiver. Store the cap and plug in a suitable location for safekeeping.
  - b. Clean the cable and port connectors (“[Clean Fiber Optic Components](#)” on page 199).
  - c. Insert the keyed LC cable connector into the port’s optical transceiver.
6. Disconnect the ESD wrist strap from the director chassis and your wrist.
7. Inspect the UPM card to ensure all amber LEDs are extinguished. If any amber LEDs are illuminated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.

8. At the Hardware View, click **Logs > Event Log**. The Event Log displays. Ensure the following event codes display in the log:

- **500**—Port card hot-insertion initiated.
- **501**—Port card has been recognized.

If an event code **501** does not display in the log, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.

9. At the Hardware View, double-click the graphic representing the replacement card to open the Port Card View. At the Port Card View:
  - a. Ensure no alert symbols display that indicate a failure (yellow triangle or red diamond).
  - b. Verify that UPM card information (FRU name, position, and state) is correct.

If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.

10. Restore communication to the replacement UPM card and set the card online as directed by the customer (“[Unblock a UPM Card](#)” on page 209). Inform the customer the UPM card is available for use.
11. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
12. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.
  - If at an EWS interface:
    - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
    - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
    - c. Click **Clear Light**.
13. If necessary, close and lock the equipment cabinet door.



## RRP: SFP Optical Transceiver

Use the following procedures to remove or replace an SFP optical transceiver from a UPM card. A list of tools required is provided.

### Tools Required

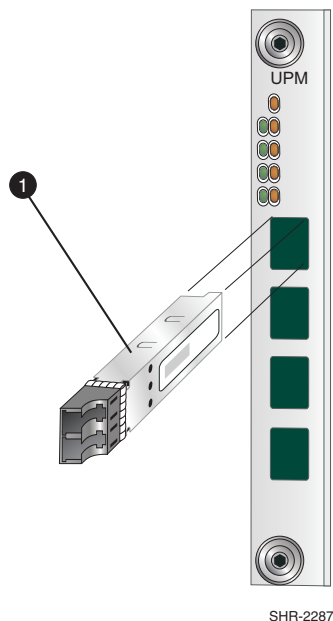
The following tools are required to perform these procedures.

- Fiber optic protective plug (provided with the director).
- Protective cap (provided with the fiber optic jumper cable).
- Fiber optic cleaning kit.

### Removing an SFP Optical Transceiver

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets the attached device offline.
2. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the customer representative.
3. Identify the defective port transceiver from the amber LED on the UPM card or failure information at the HAFM appliance's Port Card View.
4. Block communication to the port ("[Block a Port](#)" on page 207).
5. Disconnect the fiber optic jumper cable from the port:
  - a. Pull the keyed LC free from the port's optical transceiver.
  - b. Place a protective cap over the cable connector.
6. Depending on the manufacturer, the optical transceiver may have a locking mechanism to secure the transceiver in the port receptacle, or the transceiver may have a pull tab to assist in removal.
  - a. If required, disengage the locking mechanism (usually at the left side of the transceiver) by squeezing the mechanism or pushing it toward the port receptacle.
  - b. Grasp the pull tab or the optical transceiver frame and pull the transceiver (❶) from the port receptacle, as shown in [Figure 76](#).



**Figure 76: SFP optical transceiver removal and replacement**

## Replacing an SFP Optical Transceiver

To replace an SFP optical transceiver:

1. Remove the transceiver from its packaging.
2. Insert the transceiver into the port receptacle, as shown in [Figure 76](#).
3. Perform an external loopback test for the port (“[External Loopback Test](#)” on page 192). If the test fails, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
4. Reconnect the fiber optic jumper cable:
  - a. Remove the protective cap from the cable connector and the protective plug from the port’s optical transceiver. Store the cap and plug in a suitable location for safekeeping.
  - b. Clean the cable and port connectors (“[Clean Fiber Optic Components](#)” on page 199).
  - c. Insert the keyed LC cable connector into the port’s optical transceiver.

5. Inspect the UPM card with the replacement port transceiver to ensure all amber LEDs are extinguished. If any amber LEDs are illuminated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
6. At the Hardware View, click **Logs > Event Log**. The Event Log displays. Ensure an event code **510** (SFP optics card hot-insertion initiated) displays in the log.

If an event code **510** does not display in the log, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
7. Perform one of the following to verify UPM card operation:
  - At the Hardware View, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
  - At the EWS interface, open the **Switch** tab at the View panel and ensure no amber LEDs illuminate that indicate a UPM card failure. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
8. Restore communication to the port with the replacement transceiver as directed by the customer (“[Unblock a Port](#)” on page 209). Inform the customer the port is available for use.
9. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.
  - If at an EWS interface:
    - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
    - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
    - c. Click **Clear Light**.
10. If necessary, close and lock the equipment cabinet door.

## RRP: UPM Filler Blank

Use the following procedures to remove or replace a UPM filler blank. Filler blanks cover and protect unused UPM card slots in the director chassis. A list of tools required is provided.

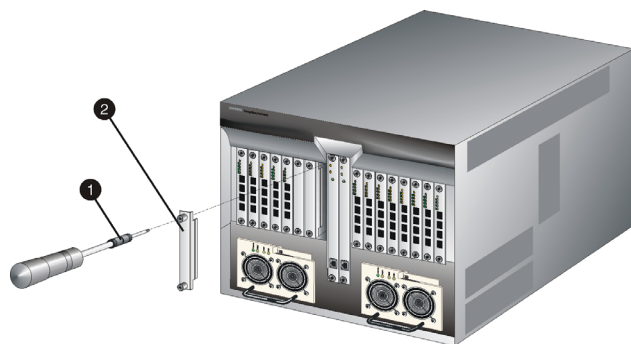
### Tools Required

The torque tool and hex adapter (provided with the director) is required to perform these procedures.

### Removing a UPM Filler Blank

To remove a filler blank:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the customer representative.
2. Identify the filler blank to be removed.
3. The filler blank is secured to the director chassis with two captive Allen screws. Both screws are spring-loaded to lock the filler blank in place.
4. Insert the torque tool (❶) into each locking Allen screw in the filler blank (❷). Turn each screw counterclockwise until the spring releases and the tool turns freely, as shown in [Figure 77](#).
5. Pull the filler blank out and remove it from the director chassis.



SHR-228E

**Figure 77: UPM filler blank removal and replacement**

## Replacing a UPM Filler Blank

To replace a filler blank:

1. Remove the filler blank from its packaging.
2. Hold the filler blank by its stiffener and insert it in the chassis card track, as shown in [Figure 77](#).
3. To secure the filler blank, sequentially insert the torque tool into each locking Allen screw. Turn each screw clockwise until you feel the torque tool release and hear a clicking sound. As each screw turns clockwise, the filler blank locks into place.
4. Verify the filler blank stiffener is flush with the front of the card cage and is even with other director logic cards.
5. If necessary, close and lock the equipment cabinet door.

## RRP: Redundant Power Supply

Use the following procedures to remove or replace a redundant power supply. A list of tools required is provided.

### Tools Required

The ESD grounding cable and wrist strap are required to perform these procedures.

### Removing a Redundant Power Supply

To remove a redundant power supply:

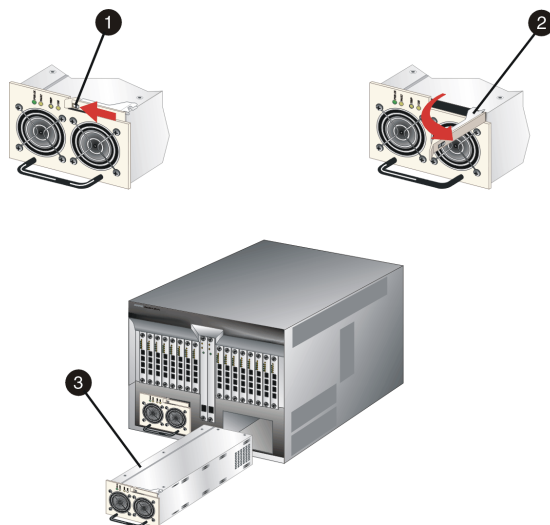
1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the customer representative.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 72](#) on page 229.



**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

3. Identify the defective power supply from the extinguished green **PWR OK** LED on the supply or failure information at the Hardware View.
4. Push the locking pin to the left (❶) to release the cam lever at the top of the power supply, as shown in Figure 78.
5. Pull the cam lever out and to the right (❷) to cam the power supply out of the director chassis.



SHR-2289

**Figure 78: Redundant power supply removal and replacement**

6. Pull the power supply (❸) from the director. Support the power supply with one hand when performing this step.
7. Place the power supply in an antistatic bag to provide ESD protection.

## Replacing a Redundant Power Supply

To replace a redundant power supply:

1. Remove the replacement power supply from its protective antistatic bag.
2. Inspect the rear of the power supply for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new power supply.

3. Orient the power supply with the cam lever disengaged and pulled out, as shown in [Figure 78](#).
  - a. Insert the power supply into the director chassis guide, then push the power supply toward the backplane to engage the connector pins.
  - b. Push the cam lever in and to the left to cam the power supply into the director chassis. Ensure the locking pin is engaged in the cam lever.
4. Disconnect the ESD wrist strap from the director chassis and your wrist.
5. Inspect the power supply to ensure the green **PWR OK** LED is illuminated and all amber LEDs are extinguished. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
6. At the Hardware View, click **Logs > Event Log**. The Event Log displays. Ensure an event code **207** (power supply installed) displays in the log.

If an event code **207** does not display in the log, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
7. Perform one of the following to verify power supply operation:
  - At the Hardware View, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
  - At the EWS interface, open the **Switch** tab at the View panel and ensure no amber LEDs illuminate that indicate a power supply failure. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
8. At the Hardware View, double-click the graphic representing the replacement power supply to open the FRU Properties dialog box. Verify that information (FRU name, position, and state) is correct. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
9. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
10. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.

- If at an EWS interface:
  - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
  - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
  - c. Click **Clear Light**.

11. If necessary, close and lock the equipment cabinet door.

## RRP: Redundant SBAR Assembly

Use the following procedures to remove or replace a redundant SBAR assembly (two assemblies in the director) with the backup SBAR assembly operational. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).

### Removing a Redundant SBAR Assembly

To remove a redundant SBAR assembly:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet rear door as directed by the customer representative.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 73](#) on page 230.



**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

3. Remove the RFI shield.

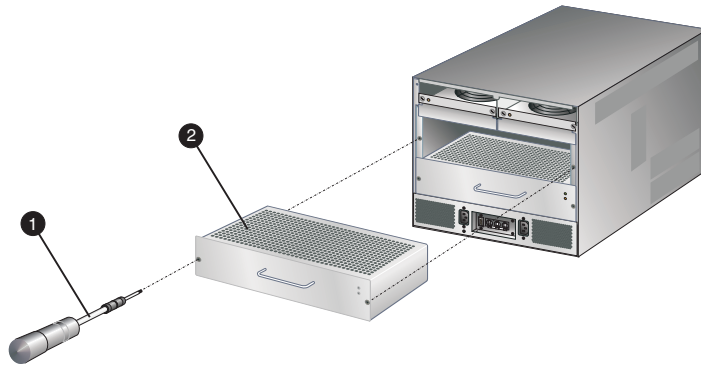


4. Identify the defective SBAR assembly from the amber LED on the assembly or failure information at the Hardware View.
5. The SBAR assembly is secured to the director backplane with two brass Allen screws. Both screws cam the assembly into and out of the backplane. Disconnect the SBAR assembly from the director backplane:



**Caution:** The torque tool supplied with the Director 2/64 is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

- a. Insert the tip of the torque tool (❶) into either brass Allen screw of the SBAR assembly (❷). Turn the screw one or two turns counterclockwise, as shown in [Figure 79](#).



**Figure 79: SBAR assembly removal and replacement**

- b. Insert the tip of the torque tool into the other brass Allen screw. Turn the screw one or two turns counterclockwise.
- c. Alternately loosen each Allen screw one or two turns until the torque tool turns freely.
6. Using the handle, pull the SBAR assembly out of the director chassis. Support the assembly with one hand when performing this step.
7. Place the SBAR assembly in an antistatic bag to provide ESD protection.

## Replacing a Redundant SBAR Assembly

To replace a redundant SBAR assembly:

1. Remove the replacement SBAR assembly from its protective antistatic bag.
2. Inspect the printed wiring assembly (PWA) side of the SBAR assembly for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new assembly.
3. Orient the SBAR assembly, as shown in [Figure 79](#). Insert the assembly into the director chassis guide, then push the assembly toward the backplane to engage the connector pins.
4. Tighten the brass Allen screws that secure the SBAR assembly to the backplane. Tighten the screws alternately to prevent binding and damage to the connector pins.
  - a. Insert the tip of the torque tool into either brass Allen screw (right or left side of the assembly). Turn the screw one or two turns clockwise. As the screw turns, that side of the assembly pulls into the backplane connector.
  - b. Insert the tip of the torque tool into the other brass Allen screw. Turn the screw one or two turns clockwise. As the screw turns, the alternate side of the assembly pulls into the backplane connector.
  - c. Alternately tighten each Allen screw one or two turns until you feel the torque tool release and hear a clicking sound.
  - d. Verify the assembly is flush and even with the other SBAR assembly in the director.
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the assembly to ensure the amber LED is extinguished. If the amber LED is illuminated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
7. At the Hardware View, click **Logs > Event Log**. The Event Log displays. Ensure the following event codes display in the log:
  - **600**—SBAR card hot-insertion initiated.
  - **601**—SBAR card hot-insertion completed.

If an event code **601** does not display in the log, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.

8. Perform one of the following to verify SBAR operation:
  - At the Hardware View, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
  - At the EWS interface, open the **Switch** tab at the View panel and ensure no amber LEDs illuminate that indicate a SBAR failure. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
9. At the Hardware View, double-click the graphic representing the replacement SBAR assembly to open the FRU Properties dialog box. Verify that information (FRU name, position, and state) is correct. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
10. Replace the RFI shield.
11. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
12. If the customer requests the replacement SBAR assembly be set as the active SBAR, perform an FRU switchover. At the Hardware View, right-click the graphic representing the replacement assembly to open a menu, then click **Switchover**.
13. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.
  - If at an EWS interface:
    - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
    - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
    - c. Click **Clear Light**.
14. If necessary, close and lock the equipment cabinet door.

## RRP: Redundant Fan Module

Use the following procedures to remove or replace a redundant cooling fan module. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.

### Removing a Redundant Fan Module

To remove a redundant fan module:

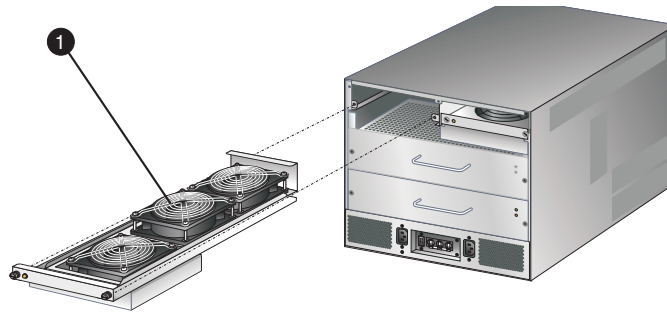
1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet rear door as directed by the customer representative.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 73](#) on page 230.



**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

3. Remove the RFI shield.
4. Identify the defective fan module from the amber LED on the module or failure information at the Hardware View.
5. Two captive screws secure the fan module (❶) to the director chassis, as shown in [Figure 80](#). Using a standard flat-tip screwdriver, loosen the captive screws.



**Figure 80: Fan module removal and replacement**



**Caution:** Do not remove a fan module unless the replacement module is available. Operation of the director with only one fan module for an extended period may cause one or more thermal sensors to post event codes.

6. Using the rear of the fan module as a handle, pull the module from the director. Support the fan module with one hand when performing this step.
7. Place the fan module in an antistatic bag to provide ESD protection.

## Replacing a Redundant Fan Module

To replace the fan module:

1. Remove the replacement fan module from its protective antistatic bag.
2. Inspect the printed wiring assembly (PWA) on the underside of the fan module for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new fan module.
3. Position the fan module at the rear of the director chassis, as shown in [Figure 80](#). Using the rear of the fan module as a handle, push the module toward the backplane to engage the connector pins. Support the fan module with one hand when performing this step.
4. Using a standard flat-tip screwdriver, tighten the two captive screws that secure the fan module to the director chassis.
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the fan module to ensure the amber LED is extinguished. If the LED is illuminated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.

7. At the Hardware View, click **Logs > Event Log**. The Event Log displays. Ensure an event code **321** (fan FRU inserted) displays in the log.  
If an event code **321** does not display in the log, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
8. Perform one of the following to verify fan module operation:
  - At the Hardware View, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
  - At the EWS interface, open the **Switch** tab at the View panel and ensure no amber LEDs illuminate that indicate a fan module failure. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
9. At the Hardware View, double-click the graphic representing the replacement fan module to open the FRU Properties dialog box. Verify that information (FRU name, position, and state) is correct. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
10. Replace the RFI shield.
11. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
12. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.
  - If at an EWS interface:
    - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
    - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
    - c. Click **Clear Light**.
13. If necessary, close and lock the equipment cabinet door.

## RRP: Power Module Assembly

Use the following procedures to remove or replace the power module assembly. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Standard flat-tip screwdriver.
- Standard cross-tip (Phillips) screwdriver.
- ESD grounding cable and wrist strap.

### Removing a Power Module Assembly

To remove the power module assembly:

1. Notify the customer the director will be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, unlock and open the cabinet front and rear doors as directed by the customer representative.
3. Power off and unplug the director ("[Power-Off Procedure](#)" on page 201).



**WARNING:** Ensure both power cords are disconnected from the power module assembly prior to removal or replacement.

---

4. Follow ESD procedures by attaching a wrist strap to an approved bench grounding point and your wrist.

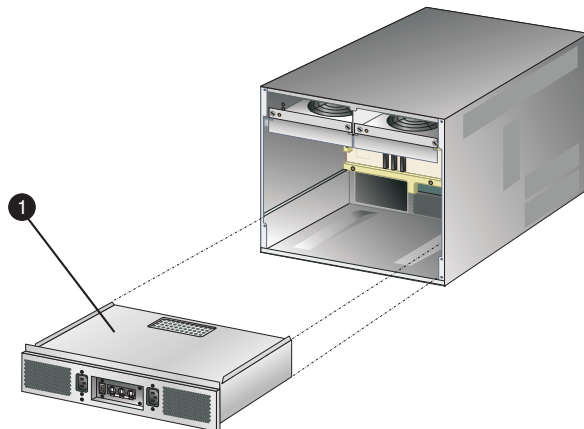


**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to an approved bench grounding point and wearing an ESD wrist strap.

---

5. Unseat and disconnect (but do not remove) both power supplies ("[RRP: Redundant Power Supply](#)" on page 245).
6. Remove the RFI shield.

7. Remove both SBAR assemblies (“[RRP: Redundant SBAR Assembly](#)” on page 248).
8. Six panhead Phillips screws (two at the top and four at the bottom) secure the power module assembly (❶) to the director chassis, as shown in [Figure 81](#). Using a standard Phillips screwdriver, loosen and remove the screws.



**Figure 81: Power module assembly removal and replacement**

9. Pull the power module assembly (with the SBAR assembly support shelf) out of the director chassis. Support the assembly with one hand when performing this step.
10. Place the power module assembly in an antistatic bag to provide ESD protection.

## Replacing a Power Module Assembly

To replace the power module assembly:

1. Remove the replacement power module assembly from its protective antistatic bag.
2. Inspect the PWA side of the power module assembly for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new assembly.
3. Position the power module assembly at the rear of the director chassis, as shown in [Figure 81](#). Push the module toward the backplane to engage the connector pins. Support the fan module with one hand when performing this step.



4. Using a standard Phillips screwdriver, insert and tighten the six panhead Phillips screws that secure the power module assembly.
5. Replace both SBAR assemblies (“[RRP: Redundant SBAR Assembly](#)” on page 248).
6. Replace the RFI shield.
7. Seat and connect both power supplies (“[RRP: Redundant Power Supply](#)” on page 245).
8. Disconnect the ESD wrist strap from the director chassis and your wrist.
9. Power on the director (“[Power-On Procedure](#)” on page 200).
10. Verify that power-on self-tests (POSTs) complete and the green power LED on the front bezel, green LED on the active CTP2 card, and green **PWR OK** LEDs on both power supplies remain illuminated. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
11. Perform one of the following to verify power module assembly operation:
  - At the Hardware View, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
  - At the EWS interface, open the **Switch** tab at the View panel and ensure no amber LEDs illuminate that indicate a power module assembly failure. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
12. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
13. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.
  - If at an EWS interface:
    - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.

- b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
  - c. Click **Clear Light**.
14. If necessary, close and lock the equipment cabinet door.

## RRP: Backplane

Use the following procedures to remove or replace the backplane. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Torque tool and hex adapter (provided with the director).
- Standard flat-tip screwdriver.
- Standard cross-tip (Phillips) screwdriver.
- ESD grounding cable and wrist strap.
- Maintenance terminal (desktop or notebook PC) with:
  - Microsoft Windows 98, Windows 2000, Windows Millennium Edition, or Windows XP.
  - RS-232 serial communication software (such as ProComm Plus or HyperTerminal). HyperTerminal is provided with Windows operating systems.
- Asynchronous RS-232 null modem cable (provided with the director).

### Removing a Backplane

To remove the backplane:

1. At the Hardware View, double-click the graphic representing the director bezel (do not click a graphical FRU) to open the Director Properties dialog box. Record the director serial number. This number must be programmed into the replacement backplane.

If the director is not communicating with the HAFM appliance (Director Properties dialog box is not available), obtain the serial number while performing [step 5](#).

2. Notify the customer the director will be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
3. If the director is installed in a stand-alone configuration, go to [step 4](#). If the director is rack-mounted, unlock and open the cabinet front and rear doors as directed by the customer representative.
4. Power off and unplug the director ("[Power-Off Procedure](#)" on page 201).



**WARNING:** Ensure both power cords are disconnected from the power module assembly prior to removal or replacement.

---

5. If necessary, record the director serial number from the silver label at the bottom front of the chassis (under the CTP2 cards).
6. Follow ESD procedures by attaching a wrist strap to an approved bench grounding point and your wrist.

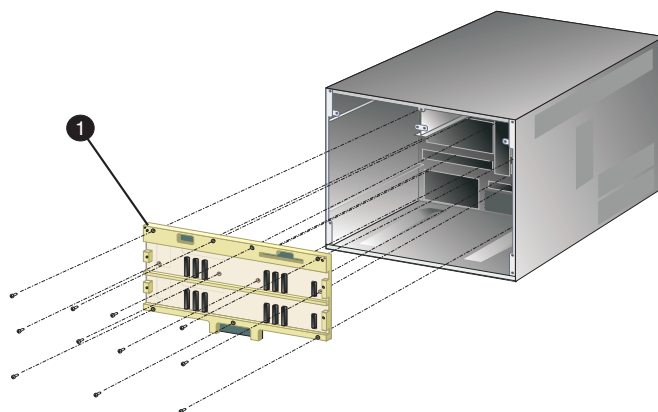


**Caution:** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to an approved bench grounding point and wearing an ESD wrist strap.

---

7. Unseat and disconnect all logic cards (CTP2 and UPM cards) from the backplane. Unseat the cards only; do not remove them from the director chassis. In addition, do not disconnect the Ethernet or fiber optic cables. For each logic card:
  - a. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the screw counterclockwise until the spring releases and the tool turns freely.
  - b. Insert the torque tool into the Allen screw at the top of the card. To unseat the card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely.
  - c. Disconnect the card from the backplane by pulling it out of the card track approximately two inches.
8. Unseat and disconnect (but do not remove) both power supplies ("[RRP: Redundant Power Supply](#)" on page 245).
9. Remove the RFI shield.

10. Remove both fan modules (“[RRP: Redundant Fan Module](#)” on page 252).
11. Remove both SBAR assemblies (“[RRP: Redundant SBAR Assembly](#)” on page 248).
12. Remove the power module assembly (“[RRP: Power Module Assembly](#)” on page 255).
13. The backplane (❶) is secured to the director chassis with 11 panhead Phillips screws, as shown in [Figure 82](#).



SHR-2307

**Figure 82: Backplane removal and replacement**

Remove the backplane:

- a. Using a standard Phillips screwdriver, loosen and remove 10 of the 11 screws that secure the backplane to the chassis. Loosen the screws alternately from bottom to top and from side to side. Leave one of the top center screws in place until ready to remove the backplane.
- b. While holding the backplane in place, loosen and remove the top center screw.
- c. Tilt the top of the backplane away from the director chassis.
- d. Remove the backplane (PWA and frame as one FRU) from the chassis. Place the backplane in an antistatic bag to provide ESD protection.

## Replacing a Backplane

To replace the backplane and all FRUs disconnected from the backplane:

1. Replace the backplane:
  - a. Remove the replacement backplane from its protective antistatic bag. Inspect the backplane PWA to ensure no connector pins are damaged.
  - b. Align the guide pins on the back of the backplane with the alignment holes in the director chassis, as shown in [Figure 82](#).
  - c. While holding the backplane in place, insert and hand tighten one of the top center panhead Phillips screws.
  - d. Insert and hand tighten the remaining 10 panhead Phillips screws. Tighten the screws alternately from bottom to top and from side to side.
  - e. Using a standard Phillips screwdriver, tighten the 11 panhead screws that secure the backplane to the chassis. Tighten the screws alternately from bottom to top and from side to side.
2. Replace the power module assembly (“[RRP: Power Module Assembly](#)” on page 255).
3. Replace both SBAR assemblies (“[RRP: Redundant SBAR Assembly](#)” on page 248).
4. Replace both fan modules (“[RRP: Redundant Fan Module](#)” on page 252).
5. Replace the RFI shield.
6. Seat and connect both power supplies (“[RRP: Redundant Power Supply](#)” on page 245).
7. Seat all logic cards (CTP2 and UPM cards) into the backplane. For each logic card:
  - a. Slide the card forward until it makes contact with the backplane.
  - b. Insert the torque tool into the Allen screw at the top of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.
  - c. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.
  - d. Verify the card stiffener is flush with the front of the card cage and is even with other director logic cards.
8. Disconnect the ESD wrist strap from the director chassis and your wrist.

9. Power on the director (“[Power-On Procedure](#)” on page 200).
10. Verify that POSTs complete and the green power LED on the front bezel, green LED on the active CTP2 card, and green **PWR OK** LEDs on both power supplies remain illuminated. If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
11. Reprogram the replacement backplane with the original director serial number:
  - a. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a flat-tip screwdriver may be required). Connect the 9-pin end of the RS-232 null modem cable to the 9-pin maintenance port on the director.
  - b. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
  - c. Power on the maintenance terminal and establish a hyperterminal connection. Use the following settings:
    - Bits per second—57600
    - Data bits—8
    - Parity—None
    - Stop bits—1
    - Flow control—HardwareWhen the parameters are set, click **OK**. The HyperTerminal window displays.
  - d. At the **C>** prompt, type the maintenance-level password (the default is **level-2**) and press **Enter**. The password is case-sensitive. The HyperTerminal window displays with a **C>** prompt at the top of the window.
  - e. Type the command `oem nnnnnnnnn`, where nnnnnnnnn is the original director serial number recorded in [step 1](#) or [step 5](#) of the removal procedure.
  - f. Click **Exit** on the **File** menu to close the *HyperTerminal* application.
12. Initial machine load (IML) the director. At the front of the director, press and hold the white IML button on the faceplate of the active CTP2 card (green LED illuminated) for three seconds.

13. At the Hardware View, observe all FRU graphics and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to “[MAP 0000: Start MAP](#)” on page 46 to isolate the problem.
14. Perform the data collection procedure (“[Collecting Maintenance Data](#)” on page 197).
15. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the *HAFM* application, open the Hardware View and:
    - a. Right-click the front panel bezel graphic (away from an FRU) to open a menu.
    - b. Click **Clear System Error Light**.
  - If at an EWS interface:
    - a. Click the **Switch** tab at the Operations panel. The Operations panel displays with the Switch page open.
    - b. Click the **Sys Err Light** tab. The Switch page displays with the **Sys Err Light** tab selected. A System Error Light is ON message displays on the page.
    - c. Click **Clear Light**.
16. If necessary, close and lock the equipment cabinet door.





# Illustrated Parts Breakdown

## 5

This chapter provides an illustrated parts breakdown for all Director 2/64 field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

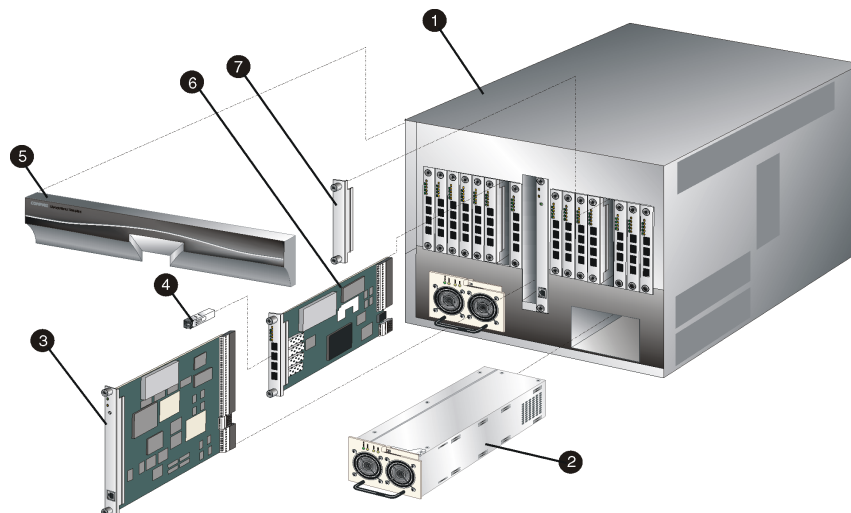
- Front-accessible FRUs
- Rear-accessible FRUs
- Miscellaneous parts

Exploded-view illustrations portray the director disassembly sequence for clarity. Illustrated FRUs are numerically keyed to associated parts lists. The parts lists also include HP part numbers, descriptions, and quantities.

An (\*ESD\*) symbol precedes the description of an FRU containing electrostatic discharge (ESD) sensitive components. Handle ESD-labelled FRUs in accordance with caution statements in this manual.

## Front-Accessible FRUs

Figure 83 illustrates front-accessible FRUs, and Table 27 is the parts list. The table includes reference numbers to Figure 83, part numbers, descriptions, and quantities.



**Figure 83: Front-accessible FRUs**

**Table 27: Front-Accessible FRU Parts List**

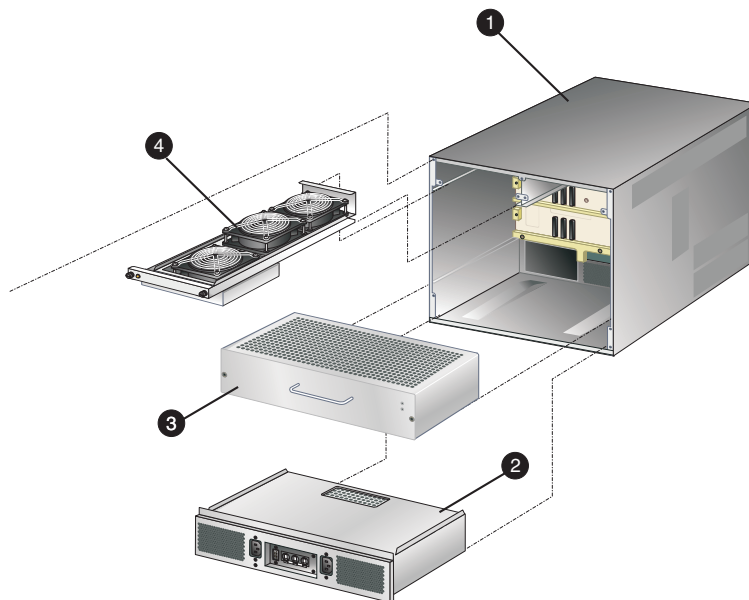
Ref.	Part Number	Description	Qty.
Ref		Base assembly, Director 2/64	
①	not procurable	Chassis assembly	1
②	254137-001	(*ESD*) Power supply, 85-264 VAC, 48 VDC	2
③	254136-001	(*ESD*) Printed wiring assembly, control processor (CTP)	2
④	300834-B21	SFP transceiver, optical, 2 Gb/s, shortwave, 500 m	0 to 64
	300835-B21	SFP transceiver, optical, 2 Gb/s, longwave, 10 km	0 to 64
	300836-B21	SFP transceiver, optical, 2 Gb/s, extended longwave, 35 km	0 to 64

**Table 27: Front-Accessible FRU Parts List (Continued)**

Ref.	Part Number	Description	Qty.
⑤	not procurable	Bezel assembly	1
⑥	316094-B21	(*ESD*) Printed wiring assembly, universal port module (UPM), 4-port, LC (with shortwave optics)	8 to 16
⑥	316094-B21	(*ESD*) Printed wiring assembly, universal port module (UPM), 4-port, LC (with longwave optics)	8 to 16
⑦	254130-001	Filler blank, UPM	0 to 8

## Rear-Accessible FRUs

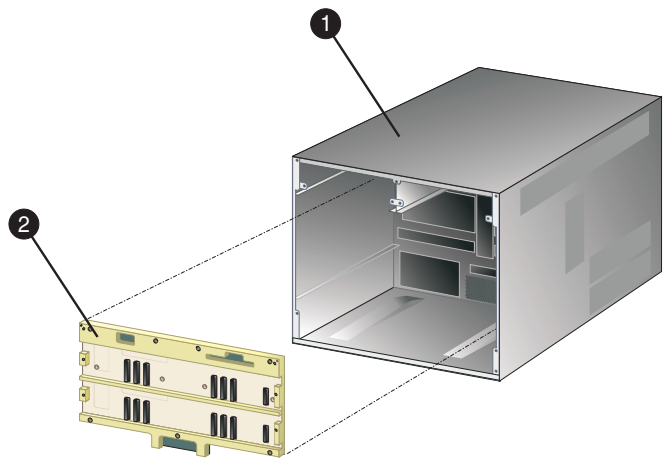
Figure 84 and Figure 85 illustrate rear-accessible FRUs, and Table 28 and Table 29 are the rear-accessible parts lists. The tables include reference numbers to Figure 84 and Figure 85, part numbers, descriptions, and quantities.



**Figure 84: Rear-accessible FRUs (part 1)**

**Table 28: Rear-Accessible FRU Parts List (Part 1)**

Ref.	Part Number	Description	Qty.
Ref		Base assembly, Director 2/64	
❶	not procurable	Chassis assembly	1
❷	254128-001	(*ESD*) Power distribution assembly	1
❸	254133-001	(*ESD*) Printed wiring assembly, serial crossbar (SBAR)	2
❹	254129-001	(*ESD*) Fan module	2



SHR-2307A

Figure 85: Rear-accessible FRUs (part 2)

Table 29: Rear-Accessible FRU Parts List (Part 2)

Ref.	Part Number	Description	Qty.
Ref		Base assembly, Director 2/64	
❶	not procurable	Chassis assembly	1
❷	254131-001	(*ESD*) Printed wiring assembly, backplane	1

## Miscellaneous Parts

[Table 30](#) is the parts list for miscellaneous parts

**Table 30: Miscellaneous Parts**

Ref.	Part Number	Description
Ref	254138-001	Power cord, 120 VAC, United States
Ref	258754-001	Power cord, AC, 5-15R
Ref	254139-001	Power cord, AC Adapter/Jumper, 2.5 m
Ref	258753-001	Adapter, ac, 100-240 VAC, autosense
Ref	254143-001	Cable, Ethernet, 10 ft
Ref	254144-001	Cable, null modem, 10 ft
Ref	254145-001	Plug, loopback, shortwave
Ref	254146-001	Plug, loopback, longwave
Ref	302659-B21	Rack mount kit, 9000, 10000, and 11000 series
Ref	339227-B21	System/e Rack mount Kit
Ref	254135-001	Screwdriver, with bit

# Information and Error Messages



This appendix lists information and error messages that display in pop-up message boxes from the HP StorageWorks *HA-Fabric Manager (HAFM)* application and the associated Element Managers.

The first section of the appendix lists *HAFM* application messages. The second section lists Element Manager messages. The text of each message is followed by a description and recommended course of action.

## HAFM Application Messages

This section lists *HAFM* application information and error messages in alphabetical order.

**Table 31: HAFM Messages**

Message	Description	Action
A zone must have at least one zone member.	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone using the Modify Zone dialog box.
A zone set must have at least one zone.	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set using the Modify Zone dialog box.
All alias, zone, and zone set names must be unique.	When creating a new alias, zone, or zone set, the name must be unique.	At the New Zone dialog box, choose a unique name for the new alias, zone, or zone set.
All zone members are logged.	Attempt was made to display all zone members not logged in using the <b>Zone Set</b> tab, but all members are currently logged in.	Informational message.
An HAFM application session is already active from this workstation.	Only one instance of the <i>HAFM</i> application is allowed to be open per remote workstation.	Close all but one of the <i>HAFM</i> application sessions.
Are you sure you want to delete this network address?	The currently-selected network address will be deleted.	Click <b>Yes</b> to delete or <b>No</b> to cancel.
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click <b>Yes</b> to delete the nickname or <b>No</b> to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click <b>Yes</b> to delete the product or <b>No</b> to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click <b>Yes</b> to delete the user or <b>No</b> to cancel the operation.



**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click <b>Yes</b> to delete the zone or <b>No</b> to cancel the operation.
Are you sure you want to delete this zone set?	The selected zone set will be deleted from the zone library.	Click <b>Yes</b> to delete the zone set or <b>No</b> to cancel the operation.
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click <b>Yes</b> to overwrite or <b>No</b> to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click <b>Yes</b> to delete the members or <b>No</b> to cancel the operation.
Cannot add a switch to a zone.	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding World Wide Name for the device you want to add to the zone.
Cannot connect to management server.	The <i>HAFM</i> application at a remote workstation could not connect to the HAFM appliance.	Verify the HAFM appliance internet protocol (IP) address is valid.
Cannot delete product.	The selected product cannot be deleted.	Verify the HAFM appliance-to-product link is up. If the link is up: <ul style="list-style-type: none"> <li>■ The HAFM appliance may be busy.</li> <li>■ Another Element Manager instance may be open.</li> <li>■ You may not have permission to delete the product.</li> </ul>
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You attempted to disable Fabric Binding through the Fabric Binding dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in the <i>HAFM</i> application before disabling Fabric Binding.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route between devices that are attached to switches or directors managed by a different HAFM appliance.	Make sure devices named in Show Routes dialog box are attached to products managed by this HAFM appliance.
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Edge Switch 2/16s, Edge Switch 2/32s, Director 2/64s, or Director 2/140s.
Cannot display route. Device is not a member of a zone in the active zone set.	You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.
Cannot display route on one switch fabric.	You cannot show routes between end devices in a fabric when configuring <b>Show Routes (Configure menu)</b> .	Error displays when attempting to show routes on a fabric with only one switch. Configure <b>Show Routes</b> on a multi-switch fabric.
Cannot display route. error 9.	An internal error has occurred while trying to view routes.	Contact the next level of support to report the problem.
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then modify the name through the Modify Zone Set dialog box.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then modify the name through the Modify Zone Set dialog box.
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM appliance-to-product link is up. If the link is up: <ul style="list-style-type: none"> <li>■ The HAFM appliance may be busy.</li> <li>■ Another Element Manager instance may be open.</li> <li>■ You may not have permission to modify the product.</li> </ul>
Cannot perform operation. Fabric is unknown.	This message displays if no switches in the fabric are connected to the HAFM appliance.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM appliance and retry the operation.
Cannot perform operation. The list of attached nodes is unavailable.	This message displays when attached nodes are unavailable and you attempt to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
Cannot save current SNMP configuration.	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.
Cannot set write authorization without defining a community name.	An SNMP community name has not been configured.	Enter a valid community name in the Configure SNMP dialog box.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Cannot show zoning library. No fabric exists.	You cannot show the zoning library if no fabric exists. You must have identified a switch or director to the <i>HAFM</i> application for a fabric to exist.	Identify an existing switch or director to the <i>HAFM</i> application using the New Product dialog box.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click <b>OK</b> to delete the log contents or <b>Cancel</b> to cancel the operation.
Connection to management server lost.	The connection to the remote HAFM appliance has been lost.	Log in to the HAFM appliance again through the HAFM Log In dialog box.
Connection to management server lost. Click OK to exit application.	The <i>HAFM</i> application at a remote workstation lost the network connection to the HAFM appliance.	Re-start the <i>HAFM</i> application to connect to the HAFM appliance.
Could not export log to file.	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Default zoning is not supported in Open Fabric Mode.	A default zone cannot be enabled when the product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers.	Change the Interop Mode from Open Fabric to Homogeneous using the Configure Fabric Parameters dialog box. You can also redefine zone members by the device WWN.
Device is not a member of a zone in the active zone set.	The selected device is not a member of a zone in the active zone set and therefore cannot communicate with the other devices in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Download complete. Click OK and start the HAFM.	Download of HAFM and the Element Manager is complete.	Start the <i>HAFM</i> application to continue.
Duplicate community names require identical write authorizations.	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
Duplicate Fabric Name.	The specified fabric name already exists.	Choose another name for the fabric.
Duplicate name in zoning configuration. All zone and zone set names must be unique.	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
Duplicate nickname in nickname configuration.	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.
Duplicate World Wide Name in nickname configuration.	A World Wide Name can be associated with only one nickname.	Modify (to make it unique) or delete the selected World Wide Name.
Duplicate zone in zone set configuration.	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.
Duplicate zone member in zone configuration.	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
Element Manager instance is currently open.	A product cannot be deleted while an instance of the Element Manager is open for that product.	Close the Element Manager, then delete the product.
Enabling this zone set will replace the currently active zone set. Do you want to continue?	Only one zone set can be active. By enabling the selected zone set, the current active zone set will be replaced.	Click <b>OK</b> to continue or <b>Cancel</b> to end the operation.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Error connecting to switch.	While viewing routes, the HAFM appliance was unable to connect to the switch. The switch failed or the switch-to-HAFM appliance Ethernet link failed.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The <i>HAFM</i> application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.
Error removing zone or zone member.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the <i>HAFM</i> application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Fabric Log will be lost once the fabric unpersists. Do you want to continue?	When you unpersist a fabric, the corresponding fabric log is deleted.	Click <b>Yes</b> to unpersist the fabric or <b>No</b> to cancel the operation.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Fabric member could not be found.	A fabric member does not exist when the application prepared to find a route, find a route node, or gather route information on that fabric member.	Ensure the product is incorporated into the fabric and retry the operation. If the problem persists, contact the next level of support.
Fabric not persisted.	You attempted to refresh or clear the log, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted.	Click <b>OK</b> to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
File transfer aborted.	You aborted the file transfer process.	Verify the file transfer is to be aborted, then click <b>OK</b> to continue.
HAFM error <error number 1 through 8 >.	The <i>HAFM</i> application encountered an internal error (1 through 8 inclusive) and cannot continue operation.	Contact the next level of support to report the problem.
Management server could not log you on. Verify your username and password.	An incorrect username or password (both case sensitive) was used while attempting to log in to the <i>HAFM</i> application.	Verify the username and password with the customer's network administrator and retry the operation.
Management server is shutting down. Connection will be terminated.	The <i>HAFM</i> application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Invalid name.	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Choose a valid name and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number. Valid ports are (0-< nn >).	You have specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus 1. For example, for a switch with 32 ports, the valid port range is 0–31.
Invalid product selection.	At the New Product dialog box, an invalid product was selected.	Choose a valid product and retry the operation.



**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Invalid request.	<p>Three conditions result in this message:</p> <ul style="list-style-type: none"> <li>■ You tried to add or modify a product from <b>Product View</b> and the network address is already in use. (Network addresses must be unique.)</li> <li>■ You tried to create a new user with a username that already exists. (A username must be unique.)</li> <li>■ You tried to delete the default Administrator user. (The default Administrator user cannot be deleted.)</li> </ul>	<p>Choose the action that is appropriate to the activity that caused the error:</p> <ul style="list-style-type: none"> <li>■ Network address: Specify a unique network address for the product.</li> <li>■ username: Specify a unique username for the new user ID.</li> <li>■ Do not delete the default Administrator user.</li> </ul>
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.
Invalid World Wide Name.	The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a World Wide Name using the correct format.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Invalid World Wide Name or nickname.	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
Invalid World Wide Name. Valid WWN format is: xx:xx:xx:xx:xx:xx:xx:xx:xx.	The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Retry the operation using a valid WWN or nickname.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.
Limit exceeded.	You cannot add a new product or user to <i>HAFM</i> application if the maximum number of that resource already exists on the system.	Delete unneeded products or users from the system, before attempting to add any new ones.
No address selected.	You cannot complete the operation because an address has not been selected.	Choose an address and retry the operation.
No attached nodes selected.	An operation was attempted without an attached node selected.	Choose an attached node and try the operation again.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
No management server specified.	An HAFM appliance is not defined to the <i>HAFM</i> application.	At the HAFM 8 Log In dialog box, type an appliance name in the <b>Server Name</b> field and click <b>Login</b> .
No nickname selected.	No nickname was selected when the command was attempted.	Choose a nickname and try again.
No Element Managers installed.	No director or switch Element Manager is installed on this workstation.	Install the appropriate Element Manager to this workstation.
No routing information available.	No information is available for the route selected.	Choose a different route and try the operation again.
No user selected.	A user was not selected when the command was attempted.	Choose a user and try again.
No zone member selected.	A zoning operation was attempted without a zone member selected.	Choose a zone member and try the operation again.
No zone selected.	A zoning operation was attempted without a zone selected.	Choose a zone and try the operation again.
No zone selected or zone no longer exists.	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Choose a zone and try the operation again.
No zone set active.	A zone set cannot be deactivated if there are no active zones.	Informational message only—no action is required.
No zone set selected.	A zoning operation was attempted without a zone set selected.	Choose a zone set and try the operation again.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
No zone set selected or zone set no longer exists.	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Choose a zone set and try the operation again.
Only attached nodes can be displayed in this mode.	You cannot display unused ports when adding ports by World Wide Name.	Change the add criteria to Add by Port.
Password and confirmation don't match.	Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
Remote sessions are not allowed from this network address.	Only IP addresses of remote workstations specified at the Remote Access dialog box are allowed to connect to the HAFM appliance.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.
Remote session support has been disabled.	The connection between the specified remote workstation and the HAFM appliance was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the Remote Access dialog box.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later.
Route data corrupted.	The information for this route is corrupt.	Try the operation again. If the problem persists, contact the next level of support.
Route request timeout.	The Show Route request timed out.	Try the operation again. If the problem persists, contact the next level of support.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
Routing is not supported by the switch.	This switch or director does not support the Show Routes feature.	Choose a different switch or director to show the route.
SANtegrity Feature not installed. Please contact your sales representative.	You selected <b>Fabric Binding</b> or <b>Enterprise Fabric Mode</b> from the <b>Fabrics</b> menu. These selections are not enabled because the optional SANtegrity binding feature is not installed.	Install the SANtegrity Binding feature to use Fabric Binding or enable Enterprise Fabric Mode.
Select alias to add to zone.	An alias was not selected before clicking <b>Add</b> .	Choose an alias before clicking <b>Add</b> .
Selection is not a World Wide Name.	The selection made is not a World Wide Name.	Choose a valid World Wide Name before performing this operation.
Server shutting down.	The <i>HAFM</i> application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Switch is not managed by HAFM.	The selected switch or director is not managed by the <i>HAFM</i> application.	Choose a different switch or director.
The Administrator user cannot be deleted.	The administrator user is permanent and cannot be deleted from the Configure Users dialog box.	Informational message only—no action is required.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but a switch already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the Add Detached Switch dialog box.
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager and cannot perform the requested operation.	Wait until the process completes, then perform the operation again.
The link to the managed product is not available.	The Ethernet connection between the HAFM appliance and managed product is down or unavailable.	Establish and verify the network connection.
The maximum number of aliases has already been configured.	The maximum number of aliases allowed was reached.	Delete an existing alias before adding a new alias.
The maximum number of management server network addresses has already been configured.	The number of HAFM appliance IP addressees that can be defined to the <i>HAFM</i> application has already been configured.	Delete an existing IP address before adding a new address.
The maximum number of members has already been configured.	The maximum number of unique members is 4097. The maximum number of members is 8192.	Delete an existing zone member before adding a new zone member.
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the <i>HAFM</i> application was reached.	Delete an existing nickname before adding a new nickname.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
The maximum number of open products has already been reached.	The maximum number of open switches allowed was reached.	Close an <i>Element Manager</i> session (existing open product) before opening a new session.
The maximum number of products has already been configured.	The number of managed HP switches (48) that can be defined to the <i>HAFM</i> application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of managed HP switches of this type (48) that can be defined to the <i>HAFM</i> application was reached.	Delete an existing product of this type before adding a new product.
The maximum number of remote network addresses has already been configured.	A maximum number of eight IP addresses for remote workstations can be configured at the Session Options dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of users has already been configured.	The number of users (32) that can be defined to the <i>HAFM</i> application was reached.	Delete an existing user before adding a new user.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.
The software version on this management server is not compatible with the version on the remote management server.	A second HAFM appliance (client) connecting to the HAFM appliance must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM appliance.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected fabric log is no longer available because the fabric has been unpersisted.	To start a new log for the fabric, persist the fabric through the Persist Fabric dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.
This product is not managed by this management server.	The product selected is not managed by this HAFM appliance.	Choose a product managed by this HAFM appliance or go to the HAFM appliance that manages the affected product.
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	You attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric.	Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected.



**Table 31: HAFM Messages (Continued)**

Message	Description	Action
This World Wide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but an entry already exists in the Fabric Membership List with the same World Wide Name (WWN).	Enter a unique World Wide Name for the switch in the Add Detached Switch dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.
You do not have a compatible version of the management server software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click OK to install a compatible version.	The <i>HAFM</i> application version running on the HAFM appliance differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM appliance.	Download a compatible version of the <i>HAFM</i> application to the remote workstation (client) using the Web install procedure.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required using the Configure Users dialog box.
You must define an SMTP server address.	An SMTP server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the Configure E-Mail dialog box.
You must define at least one E-mail address.	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the Configure E-Mail dialog box.

**Table 31: HAFM Messages (Continued)**

Message	Description	Action
You must define at least one remote network address.	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the Remote Access dialog box.
You must download the HAFM client via the web install.	An attempt was made to download the <i>HAFM</i> application to a remote workstation (client) using an improper procedure.	Download a compatible version of the <i>HAFM</i> application to the remote workstation (client) using the Web install procedure.
Zones configured with port numbers are ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names.	Informational message only—no action is required.
Zones must be defined before creating a zone set.	You cannot create a zone set without any zones defined for <i>HAFM</i> .	Define zones using the New Zone dialog box.
Zoning by port number is ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names.	Informational message only—no action is required.
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if <i>HAFM</i> is in Open Fabric Mode.	Either define zones by WWN of device or change to Homogeneous Fabric mode in the Configure Operation Mode dialog box of the Element Manager.
Zoning name already exists.	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

## Element Manager Messages

This section lists Element Manager information and error messages in alphabetical order.

**Table 32: Element Manager Messages**

Message	Description	Action
A Preferred Path already exists between this Source Port and this Destination Domain ID. Please re-configure the desired path.	For any source port, only one path may be defined to each destination domain ID.	On the Add/Change Preferred Path dialog box, change the preferred path.
Activating this configuration will overwrite the current configuration.	Confirmation to activate a new address configuration.	Click <b>Yes</b> to confirm activating the new address configuration or <b>No</b> to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue?	Occurs when FPM cards are installed in the director and director speed is being set to 2 Gb/sec in the Configure Switch Parameters dialog box.	Replace FPM cards with UPM cards (UPM cards operate at 1 and 2 Gb/sec) or set the director speed to 1 Gb/sec.
All port names must be unique.	A duplicate Fibre Channel port name was configured. All port names must be unique.	Reconfigure the Fibre Channel port with a unique name.
All port names must be unique.	A duplicate port name was entered. Every configured port name must be unique.	Reconfigure the port with a unique name.
An Element Manager instance is already open.	Only one instance of the Element Manager can be open at one time.	Close the open Element Manager so the desired instance of the Element Manager can be opened.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Another Element Manager is currently performing a firmware install.	Only one instance of the Element Manager can install a firmware version to the director at a time.	Wait for the firmware installation process to complete and try the operation again.
Are you sure you want to delete firmware version?	This message requests confirmation to delete a firmware version. Firmware library can store up to 8 firmware versions.	Click <b>Yes</b> to delete the firmware version or <b>No</b> to abort the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click <b>Yes</b> to confirm the deletion of the address configuration or <b>No</b> to cancel the operation.
Are you sure you want to send firmware version?	This message requests confirmation to send a firmware version from the HAFM appliance's firmware library to the director. Firmware library can store up to 8 firmware versions.	Click <b>Yes</b> to send the firmware version or <b>No</b> to abort the operation.
Cannot change Port Type while Management Style is FICON without SANtegrity feature. Please contact your sales representative.	Firmware is below the required level and you attempted to change a port type in the Configure Ports dialog box while FICON management style, but the optional SANtegrity Binding feature is not installed.	Informational message. If the firmware is below the required level, install SANtegrity Binding before changing port types in the Configure Ports dialog box while in FICON management style.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	You attempted to disable Switch Binding through the Switch Binding Change State dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the <i>HAFM</i> application or set the switch offline before you can disable Switch Binding.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Cannot disable Insistent Domain ID while Fabric Binding is active.	You attempted to disable the Insistent Domain ID parameter through the Configure Switch Parameters dialog box, but Fabric Binding is enabled.	Disable Fabric Binding through the Fabric Binding dialog box before disabling these parameters.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.
Cannot enable beaconing while the system light is on.	Occurs when choosing Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on an operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Select <b>Clear System Error Light</b> from <b>Product</b> menu to clear error light, then enable beaconing.
Cannot enable Open Trunking while Enterprise Fabric Mode is active and the switch is offline.	Enterprise Fabric mode is active and the switch or director is online and you attempted to enable Open Trunking. This message only displays if the optional Open Trunking feature is installed.	Perform either of the following steps: <ul style="list-style-type: none"> <li>■ Disable Enterprise Fabric Mode option by selecting the appropriate fabric in the Fabric Tree portion of the <b>HAFM Manager</b> window (Fabrics tab) and then selecting <b>Enterprise Fabric Mode</b> from the Fabrics menu. When the Enterprise Fabric Mode dialog box displays, click <b>Start</b> and follow prompts to disable the feature.</li> <li>■ Set the switch or director offline through the Set Online State dialog box. Display this dialog box by selecting <b>Set Online State</b> from the <b>Element Manager Maintenance</b> menu.</li> </ul>

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Cannot have E-Ports if Management Style is FICON unless SANtegrity feature is installed. Please contact your sales representative.	Firmware is below the required level and you attempted to change management style from Open Systems to FICON management style with E_Ports configured, but SANtegrity Binding is not installed.	Informational message. If firmware is below the required level and you install SANtegrity Binding before changing to FICON management style, then E_Ports will remain as E_Ports when you change to FICON management style. If SANtegrity Binding is not installed, setting a director to FICON management style will change all E_ports to G_Ports.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot install firmware to a director with a failed CTP card.	A firmware version cannot be installed on a director with a failed control processor (CTP) card.	Replace the failed CTP card and retry the firmware installation.
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a switch with a defective CTP card.	Note that the CTP card is not a FRU. If it fails, the switch must be replaced. After replacement, retry the firmware install to the switch.
Cannot modify director/switch speed. Ports speeds cannot be configured at a higher data rate than the director/switch speed.	Port speeds cannot be configured at a higher data rate than the director speed. This message displays when you set director speed to 1 GB/sec through the Configure Switch Parameters dialog box and at least one of the ports is running at 2 Gb/sec.	Either return the director speed to 2 Gb/sec or configure all port data speeds to 1 Gb/sec through the Configure Ports dialog box.
Cannot perform this operation while the switch is offline.	This operation cannot take place while the director or switch is offline.	Configure the director or switch offline through the Set Offline State dialog box and then retry the operation.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Cannot retrieve current SNMP configuration.	The director SNMP configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve diagnostics results.	Director diagnostic results cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve information for port.	Port information cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port configuration.	The port configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port statistics.	Port statistics cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch date and time.	The director or switch date and time cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch state.	The director or switch state cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Cannot run diagnostics on a port that is failed.	Port diagnostics (loopback tests) cannot be performed on a port that has failed any previous diagnostic (power-on diagnostic, online diagnostic, or loopback test). The amber LED associated with the port illuminates to indicate the failed state.	Reset the port and perform diagnostics again.
Cannot run diagnostics on an active E-port.	Port diagnostics cannot be performed on an active E-port.	Run diagnostics on an E-port only when it is not active.
Cannot run diagnostics on a port that is not installed.	Port diagnostics cannot be performed on a port card that is not installed.	Run diagnostics only on a port that is installed.
Cannot run diagnostics on a port card that is not installed.	Port diagnostics (loopback tests) cannot be performed on a port that does not have a small form factor (SFF) optical transceiver installed.	Install a transceiver in the port and perform diagnostics again.
Cannot run diagnostics while a device is logged-in to the port.	Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in.	Ensure the device is logged out and perform diagnostics again.
Cannot run diagnostics while a device is logged-in to the port.	A device is logged in to the port where a diagnostic test is attempted.	Log out the device and run the diagnostic test again.
Cannot save IPL configuration while active=saved is enabled.	You cannot save the IPL file while the active=saved property is set.	The FICON Management Server property, active=save, must be disabled for HAFM to save the IPL file.



**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Cannot save port configuration.	The port configuration cannot be saved at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot save SNMP configuration.	The SNMP configuration cannot be saved at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set all ports to 1 Gb/sec due to speed restriction on some ports.	Displays if you try to set ports to operate at 1 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one configuration.
Cannot set all ports to 2 Gb/sec due to speed restriction on some ports.	Displays if you try to set ports to operate at 2 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one configuration.
Cannot set all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set Fibre Channel parameters.	Fibre Channel parameters for the director cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Cannot set switch date and time.	The switch date and time cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch state.	The director or switch state cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set write authorization without defining a community name.	A community name was not defined in the Configure SNMP dialog box for the write authorization selected.	Provide a name in the <b>Name</b> field where write authorization is checked.
Cannot start data collection.	The data collection procedure cannot be started by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot start firmware install while CTP synchronization is in progress.	The director's CTP cards are synchronizing and firmware cannot be installed until synchronization is complete.	Install the firmware after CTP card synchronization completes.
Cannot start port diagnostics.	Port diagnostics cannot be started at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot swap an uninstalled port.	A port swap cannot be performed when the port card is not installed.	Perform a swap only on a port that is installed.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click <b>OK</b> to delete the log contents or click <b>Cancel</b> to cancel the operation.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Connection to management server lost. Click OK to exit application.	The <i>HAFM</i> application at a remote workstation lost the network connection to the HAFM appliance.	Start the <i>HAFM</i> application to connect to the HAFM appliance.
Continuing may overwrite host programming. Continue?	Configurations sent from the host may be overwritten by HAFM.	Continuing will activate the current configuration, which may have been configured by a FICON host.
Could not export log to file.	A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	Ensure file name and drive are correct.
Could not find firmware file.	Firmware file selected was not found in the FTP directory. Or, the selected file is not a firmware file.	Ensure file name and directory are correct. Or, obtain a valid firmware file from your service representative.
Could not remove dump files from server.	Dump files could not be deleted from the HAFM appliance because the link may be down, or the HAFM appliance or Element Manager is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not stop port diagnostics.	Port diagnostics could not be stopped by the Element Manager because the Ethernet link is down or busy, or because the director is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not write firmware to flash.	A firmware version could not be written from the HAFM appliance to FLASH memory	Retry the operation again. If the condition persists, contact the next level of support.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Control Unit Port (CUP) name and port name are identical (FICON ONLY).	Within the address configuration, one or more of the port names are the same as the CUP name.	Make sure all names are unique for the ports and CUP name.
Date entered is invalid.	The date is entered incorrectly at the Configure Date and Time dialog box. Individual field entries may be correct, but the overall date is invalid (for example, a day entry of 31 for a 30-day month).	Verify each entry is valid and consistent.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Port diagnostics (loopback tests) cannot be performed on a port while an attached device application is running.	Terminate the device application and perform diagnostics again.
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	You attempted to remove a device WWN from the Switch Membership List (SANtegrity Binding feature) while Switch Binding is enabled.	Remove the device from the switch by blocking the port, setting the switch offline, or disabling Switch Binding through the Switch Binding Change State dialog box before removing devices from the Switch Membership List.
Director clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Director must be offline to configure.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through HAFM and you attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box.	Click <b>Yes</b> if you want to continue and disable Fabric Binding.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through the HAFM and user attempted to disable Insistent Domain ID in the <b>Configure Switch Parameters</b> dialog box.	Click <b>Yes</b> if you want to continue and disable Fabric Binding.
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	You attempted to disable Switch Binding through the Switch Binding State Change dialog box, but Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Switch Binding.
Do you want to continue with IPL?	This message requests confirmation to initial program load (IPL) the director.	Click <b>Yes</b> to IPL the director or <b>Cancel</b> to cancel the operation.
Domain IDs must be in the range of 1 to 31.	Domain IDs entered in the Configure Preferred Paths dialog box must fall in a specific range.	In the Configure Preferred Paths dialog box, change the number in the <b>Destination Domain ID</b> field to a number between 1 and 31, inclusive.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Duplicate Community names require identical write authorizations.	Duplicate community names are entered at the Configure SNMP dialog box, and have different write authorizations.	Delete the duplicate community name or make the write authorizations consistent.
Element Manager error <number>.	The Element Manager encountered an internal error and cannot continue.	Contact the next level of support to report the problem.
Element Manager instance is currently open.	A Element Manager window is currently open.	Informational message only.
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCNs. Do you want to continue?	You attempted to disable these parameters in the Configure Switch Parameters dialog box while the switch was online, but Enterprise Fabric Mode (SANtegrity Binding feature) is enabled.	Click <b>Yes</b> if you want to continue, and disable Enterprise Fabric Mode.
Error retrieving port information.	An error occurred at the Element Manager while retrieving port information because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error retrieving port statistics.	An error occurred at the Element Manager while retrieving port statistics because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error stopping port diagnostics.	An error occurred at the Element Manager while attempting to stop port diagnostics from running because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the Element Manager. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Feature not supported. The 'product name' must be running version 05.00.00 or higher.	The firmware version on the hardware product (switch or director) is lower than 05.00.00. This message only displays if the optional Open Trunking feature is installed.	Install firmware version 5.00.00 or higher on the hardware product.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the Data field.
Field has exceeded maximum number of characters.	The maximum number of data entry characters allowed in the field was exceeded.	Enter the information using the prescribed number of characters.
File transfer aborted.	You aborted the file transfer process.	Information message only.
File transfer is in progress.	A firmware file is being transferred from the HAFM appliance hard drive, or a data collection file is being transferred to a CD.	Informational message only—no action is required.
Firmware download timed out.	The director or switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file I/O error.	A firmware download operation aborted because a file I/O error occurred.	Retry the operation. If the problem persists, contact the next level of support.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Firmware file not found.	The firmware version is not installed (or was deleted) from the firmware library at the HAFM appliance.	Add the firmware version to the library and retry the operation.
Incompatible configuration between management style and management server.	If the Firmware is below the required level, only FICON management style is allowed if the FICON Management Server feature is enabled. You attempted to enable Open Systems management style.	Disable FICON Management Server, enable the Open Systems Management Server, or enable the Open Systems management style.
Incorrect product type.	When configuring a new product through the New Product dialog box, an incorrect product was specified.	Choose the correct product type for the product with the network address.
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM appliance will be lost momentarily, but Fibre Channel traffic will not be affected.	Click <b>Yes</b> to install the feature key or <b>No</b> to not install.
Internal file transfer error received from director.	The director or switch detected an internal file transfer error.	Retry the operation. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the Data field.	Remove invalid characters from the entry.



**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens, and underscores.
Invalid feature key.	The feature key was not recognized.	Re-enter the feature key. Ensure that you type each character in the correct case (upper or lower), include the dashes, and do not add any spaces at the end.
Invalid firmware file.	The file selected for firmware download is not a firmware version file.	Choose the correct firmware version file and retry the operation.
Invalid management server address.	The IP address specified for the HAFM appliance is unknown to the domain name server (invalid).	Verify and enter a valid HAFM appliance IP address.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port address.	Invalid port address has been entered.	Verify port address through the Configure Addresses—"Active" dialog box (FICON management style only) and re-enter.
Invalid port number.	The port number must be within a range of ports for the specific director or switch model.	Enter a port number within the correct range.
Invalid port swap.	Port swap selection is not allowed.	Ensure that each port selected for swap has not been previously swapped.
Invalid response received from switch.	An error occurred at the switch during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Invalid response received from director.	An error occurred at the director during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
Invalid serial number for this feature key.	The serial number and the feature key did not match.	Ensure that the feature key being installed is specifically for this director serial number.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number from 1 through 65535.
Invalid value for BB_Credit.	At the Configure Fabric Parameters dialog box, the buffer-to-buffer credit (BB_Credit) value must be an integer from 1 through 60 inclusive.	Verify and enter a valid number between 1 through 60.
Invalid value for Low BB Credit threshold (1-99) %.	<b>Low BB Credit Threshold</b> field in Configure Open Trunking dialog box must have entries in the range from 1 and 99. This message only displays if the optional Open Trunking feature is installed.	Enter a value from 1 to 99 into the <b>Low BB Credit Threshold</b> field of the Configure Open Trunking dialog box.
Invalid value for day (1-31).	At the Configure Date and Time dialog box, the DD value (day) must be an integer from 1 through 31 inclusive.	Verify and enter a valid date.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Invalid value for E_D_TOV.	At the Configure Fabric Parameters dialog box, the error detect time-out value (E_D_TOV) must be an integer from 2 through 600 inclusive.	Verify and enter a valid number.
Invalid value for hour (0-23).	At the Configure Date and Time dialog box, the HH value (hour) must be an integer from 0 through 23 inclusive.	Verify and enter a valid time.
Invalid value for minute (0-59).	At the Configure Date and Time dialog box, the MM value (minute) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.
Invalid value for month (1-12).	At the Configure Date and Time dialog box, the MM value (month) must be an integer from 1 through 12 inclusive.	Verify and enter a valid date.
Invalid value for R_A_TOV.	At the Configure Fabric Parameters dialog box, the resource allocation time-out value (R_A_TOV) must be an integer from 10 through 1200 inclusive.	Verify and enter a valid number.
Invalid value for second (0-59).	At the Configure Date and Time dialog box, the SS value (second) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Invalid value for threshold (1-99)%.	Value entered for each port in the Configure Open Trunking dialog box must be in the range from 1 to 99. This message only displays if the optional Open Trunking feature is installed.	Enter a number from 1 to 99 into the <b>Threshold %</b> column of the Configure Open Trunking dialog box.
Invalid value for year.	At the Configure Date and Time dialog box, the YYYY value (year) must be a four-digit value.	Verify and enter a four-digit value for the year.
Invalid World Wide Name or nickname.	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
Link dropped.	The HAFM appliance-to-director Ethernet link was dropped.	Retry the operation. Link re-connects are attempted every 30 seconds. If the condition persists, contact the next level of support.
Log is currently in use.	Access to the log is denied because the log was opened by another instance of the Element Manager.	Retry the operation later. If the condition persists, contact the next level of support.
Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue.	External loopback diagnostics require an optical loopback plug to be installed.	Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Maximum number of versions already installed.	The number of firmware versions that can be defined to the <i>HAFM</i> application's firmware library (eight) was reached.	Delete an existing firmware version before adding a new version.
No file was selected.	Action requires the selection of a file.	Select a file.
No firmware version file was selected.	A file was not selected in the Firmware Library dialog box before an action, such as modify or send was performed.	Click on a firmware version in the dialog box to select it, then perform the action again.
No firmware versions to delete.	There are no firmware versions in the firmware library to delete, therefore the operation cannot be performed.	Informational message only—no action is required.
Nonredundant director must be offline to install firmware.	For directors, if the director has only one CTP card, the director must be set offline to install a firmware version.  For switches, since the switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU.	Set the director or switch offline and install the firmware.
Not all of the optical transceivers are installed for this range of ports.	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Open Trunking is not installed for this product. Please contact your sales representative.	The Open Trunking feature key has not been enabled. This message only displays if the optional Open Trunking feature is installed.	Enter the feature key into the Configure Feature Key dialog box and enable the key. If you require a feature key, see your account representative.
Performing this operation will change the current state to Offline.	This message requests confirmation to set the director offline.	Click <b>OK</b> to set the director offline or click <b>Cancel</b> to cancel the operation.
Performing this operation will change the current state to Online.	This message requests confirmation to set the director online.	Click <b>OK</b> to set the director online or click <b>Cancel</b> to cancel the operation.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the Configure Date and Time dialog box, that the new time or date will overwrite the existing time or date set for the director or switch.	Verify that you want to overwrite the current date or time.
Periodic Date/Time synchronization must be cleared.	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click <b>Periodic Date/Time Synchronization</b> check box in Configure Date and Time dialog box ( <b>Configure</b> menu) to clear check mark and disable periodic date/time synchronization.
Port binding was removed from attached devices that are also participating in Switch Binding.	Informational message. You removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
Port cannot swap to itself.	Port addresses entered in the Swap Ports dialog box are the same.	Ensure that address in the first and second <b>Port Address</b> fields are different.
Port diagnostics cannot be performed on an inactive port.	This displays when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.
Port speeds cannot be configured at a higher rate than the director speed.	This displays when you configure a port to 2 Gb/sec and the director speed is set to 1 Gb/sec.	Set the director speed to 2 Gb/sec in the Configure Switch Parameter dialog box.
Port numbers must be in the range of 0 to xxx.	When configuring Preferred Paths, source ports and exit ports must be in the range of ports for the switch being configured.	In the Configure Preferred Paths dialog box, change the numbers in the <b>Source Port</b> and <b>Exit Port</b> fields to fall within the port count of the switch on which you are configuring paths.
Preferred Paths can not be enabled until the Domain ID is set to Insistent. Disable Preferred Paths, then configure Switch Parameters.	If the switch's domain ID has not been set to Insistent, the user is not allowed to activate the Preferred Path configuration with the Enable Preferred Paths check box selected.	Close the Configure Preferred Paths dialog box and click <b>Configure &gt; Operating Parameters &gt; Switch Parameters</b> . In the Configure Switch Parameters dialog box, click the <b>Insistent</b> check box.
R_A_TOV must be greater than E_D_TOV.	R_A_TOV must be greater than E_D_TOV.	Change one of the values so that R_A_TOV is greater than E_D_TOV
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the Ethernet connection between the HAFM appliance and the director is up or available.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
SANtegrity Feature not installed. Please contact your sales representative.	You selected <b>Switch Binding</b> from the <b>Configure</b> menu, but the optional SANtegrity Binding feature is not installed.	Install the SANtegrity Binding key through the Configure Feature Key dialog box before using Switch Binding features.
Send firmware failed.	A firmware download operation failed.	Retry the firmware download operation. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and <b>Stop</b> was selected on the Port Diagnostics dialog box. Diagnostics quit for the port for some reason, but the <b>Stop</b> button remains enabled.	Verify port operation. Retry diagnostics for the port and choose <b>Stop</b> from the dialog box. If problem persists, contact the next level of support.
Stop diagnostics failed. The test was not running.	This action failed because the test was not running.	Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the director's Switch Membership List (SANtegrity Binding feature), but you should note that one or more of these devices still has security control in port binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the Configure Ports dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switches with failed ports	Replace failed ports.



**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
The add firmware process has been aborted.	You aborted the process to add a firmware version to the HAFM appliance's firmware library.	Verify the firmware addition is to be aborted, then click <b>OK</b> to continue.
Switch clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and user is attempting to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
The data collection process failed.	An error occurred while performing the data collection procedure.	Try the data collection procedure again. If the problem persists, contact the next level of support.
The data collection process has been aborted.	You aborted the data collection procedure.	Verify the data collection procedure is to be aborted, then click <b>OK</b> to continue.
The default zone must be disabled to configure.	The message displays when you attempted to change the management style to Open Fabric and the default zone is enabled.	Disable the default zone and repeat the operation.
The Ethernet link dropped.	The Ethernet connection between the HAFM appliance and the director is down or unavailable.	Establish and verify the network connection.
The firmware file is corrupted.	A firmware version file is corrupt.	Contact the next level of support to report the problem.
The firmware version already exists.	This firmware version already exists in HAFM appliance's firmware library.	Informational message only—no action is required.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCNs.	You attempted to disable these parameters in the Configure Switch Parameters dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in HAFM, then disable the parameters.
The link to the director is not available.	The Ethernet connection between the HAFM appliance and the director is down or unavailable.	Establish and verify the network connection.
The link to the switch is not available.	The Ethernet connection between the HAFM appliance and the switch is down or unavailable.	Establish and verify the network connection.
The IPL configuration cannot be deleted.	Deletion of the IPL address configuration was attempted and was not allowed.	Cancel the operation.
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager, and cannot perform the requested operation.	Wait until the process is completes, then perform the operation again.
The optical transceiver is not installed.	Information is not available for a port without an optical transceiver installed.	Install an SFP optical transceiver in the port.
The switch did not accept the request.	The director or switch cannot perform the requested action.	Retry the operation. If the condition persists, contact the next level of support.
The maximum number of address configurations has been reached.	The maximum number of saved address configurations has been reached.	Delete configurations no longer needed to allow new configuration to be saved.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
The switch did not respond in the time allowed.	While waiting to perform a requested action, the director or switch timed out.	Retry the operation. If the condition persists, contact the next level of support.
The switch is busy saving maintenance information.	The director or switch cannot perform the requested action because it is busy saving maintenance information.	Retry the operation later. If the condition persists, contact the next level of support.
The switch must be offline to change the Management Style.	The firmware is below the required level and you attempted to change the management style.	Choose <b>Set Online State</b> from the <b>Maintenance</b> menu and click <b>Set Offline</b> . Then change the management style. Set the director or switch back online when finished.
The switch must be offline to configure.	A configuration changed was attempted for a configuration requiring offline changes.	Take the appropriate actions to set the director or switch offline before attempting the configuration change.
This feature is not installed. Please contact your sales representative.	This feature has not been installed.	Contact your sales representative.
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the switch offline through the Set Online State dialog box, then activate the new feature key using the Configure Feature Key dialog box.  The new feature key will display both the new features and the features that were installed previously.

**Table 32: Element Manager Messages (Continued)**

Message	Description	Action
This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?	The feature set currently installed for this system contains features that are not being installed with the new feature key.	Click <b>Yes</b> to activate the feature key and remove current features not in the new feature set or <b>No</b> to cancel.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported on firmware earlier than 01.03.00.	Informational message.
Unable to change incompatible firmware release.	You tried to download a firmware release that is not compatible with the current product configuration.	Refer to the product release notes or contact the next level of support to report the problem.
Unable to save data collection file to destination.	The HAFM appliance could not save the data collection file to the specified location (PC hard drive, CD, or network).	Retry the operation. If the condition persists, contact the next level of support.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.





# Event Code Tables

## B

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Events are reported as event codes.

This appendix lists all three-digit Director 2/64 event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format, and are grouped as follows:

- **000 through 199**—system events
- **200 through 299**—power supply events
- **300 through 399**—fan module events
- **400 through 499**—control processor (CTP) card events
- **500 through 599**—fiber port module (UPM) card events
- **600 through 699**—serial crossbar (SBAR) assembly events
- **800 through 899**—thermal events

Events are recorded in the Director 2/64 Event Log at the HAFM appliance, in the Event Log of the Embedded Web Server interface, at a remote workstation if e-mail and call-home features are enabled, at a Simple Network Management Protocol (SNMP) workstation, or at a host console if inband management is enabled. An event may also illuminate the system error light-emitting diode (LED) on the director front bezel.

In addition to numerical event codes, the tables in this appendix also provide:

- **Message**—a brief text string that describes the event.

- **Severity**—a severity level that indicates event criticality as follows:
  - Informational
  - Minor
  - Major
  - Severe (not operational)
- **Explanation**—a complete explanation of what caused the event.
- **Action**—the recommended course of action (if any) to resolve the problem.
- **Event Data**—supplementary event data (if any) that displays in the Event Log in hexadecimal format.
- **Distribution**—check marks in associated fields indicate where the event code is reported (director, HAFM appliance, or host).



## System Events (000 through 199)

Event Code: 001							
Message:	System power-down.						
Severity:	Informational.						
Explanation:	The director was powered off or disconnected from the facility AC power source. The event code is distributed the next time the director powers on, but the date and time of the code reflect the power-off time.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 010							
Message:	Login Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP2 card reset or replacement, the Login Server attempted to acquire an up-to-date copy of its databases from the other CTP2 card, but failed. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP2 card failover or replacement, initial machine load (IML), or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 020							
Message:	Name Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP2 card reset or replacement, the Name Server attempted to acquire an up-to-date copy of its databases from the other CTP2 card, but failed. All Fabric Services databases are initialized to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP2 card failover or replacement, IML, or firmware download, the Name Server database failed its CRC validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the Element Manager are allowed.						
Action:	Add the community name to the SNMP configuration using the Element Manager.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 050							
Message:	Management server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP2 card reset or replacement, the HAFM appliance attempted to acquire an up-to-date copy of its databases from the other CTP2 card, but failed. All Management Services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the HAFM appliance.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 051							
Message:	Management server database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP2 card failover or replacement, IML, or firmware download, the HAFM appliance database failed its CRC validation. All Management Services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the HAFM appliance.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 052							
Message:	Management server internal error, asynchronous status report activation, or mode register update occurred.						
Severity:	Informational.						
Explanation:	An internal operating error was detected by the HAFM appliance subsystem, an asynchronous status was reported to an attached host, or a mode register update occurred.						
Action:	HAFM appliance internal error: Perform the data collection procedure and return the backup CD to HP Services support personnel. Asynchronous status report activation: No action required. Mode register update: No action required.						
Event Data:	Supplementary data consists of reporting tasks of type eMST_SB2, with component_id eMSCID_SB2_CHPGM. For each type of error or indication, the subcomponent_id is: HAFM appliance internal error: subcomponent_id is eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR or eMS_ELR_SB2_MSG_PROCESSING_ERROR. Asynchronous status report activation: subcomponent_id is eSB2_CP_RER_ASYNCH_STATUS_REPORTING. Mode register update: subcomponent_id is eMS_ELR_MODE_REGISTER_UPDATE.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓			✓	

Event Code: 060							
Message:	Fabric Controller unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP2 card reset or replacement, the Fabric Controller attempted to acquire an up-to-date copy of its databases from the other CTP2 card, but failed. All Fabric Controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 061							
Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP2 card failover or replacement, IML, or firmware download, the Fabric Controller database failed its CRC validation. All Fabric Controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 062							
Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (director or switch) traverses more than three interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two directors or switches traverses no more than three ISLs.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) more than seven hops away. Bytes 1–3 = reserved.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The fabric element (director or switch) whose domain ID is indicated in the event data has too many ISLs attached, and that element is unreachable from this director.						
Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) with too many ISLs. Bytes 1–3 = reserved.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 070							
Message:	E_Port is segmented.						

Severity:	Informational.
Explanation:	A director E_Port recognized an incompatibility with an attached fabric element (director or switch), preventing the director from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic (data from attached devices), but transmits Class F traffic (management and control data from the attached director or switch). Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters. Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the Director 2/64 and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p>2 = Duplicate domain ID. The Director 2/64 has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations. The same name is applied to a zone for the Director 2/64 and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p>4 = Build fabric protocol error. A protocol error was detected during incorporation of the Director 2/64 into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p> <p>6 = No response from attached switch (hello timeout). The Director 2/64 periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the backup CD to HP support personnel.</p> <p style="text-align: right;">Continued</p>



Event Code: 070 (Continued)							
Event Data (Continued):	7 = ELP retransmission failure timeout. A Director 2/64 that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple exchange link protocol (ELP) frames to a fabric element (director or switch). However, because of the problem, the director did not receive responses to the ELP frames, and did not receive a fabric login (FLOGI) frame. After five ELP transmission attempts, the director E_Port (failed director) times out and segments. Go to <a href="#">“MAP 0000: Start MAP”</a> on page 46 to perform hardware fault isolation at the failed director.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 071	
Message:	Director is isolated.
Severity:	Informational.
Explanation:	The director is isolated from other fabric elements (directors or switches). This event code is accompanied by one or more 070 event codes. Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters. Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the Director 2/64 and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p>2 = Duplicate domain ID. The Director 2/64 has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations. The same name is applied to a zone for the Director 2/64 and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p>

Event Code: 071 (Continued)							
Event Data (Continued):	<p>4 = Build fabric protocol error. A protocol error was detected during incorporation of the Director 2/64 into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p> <p>5 = No principal switch. No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p>6 = No response from attached switch (hello timeout). The Director 2/64 periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the backup CD to HP support personnel.</p> <p>7 = ELP retransmission failure timeout. A Director 2/64 that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple ELP frames to a fabric element (director or switch). However, because of the problem, the director did not receive responses to the ELP frames, and did not receive an FLOGI frame. After five ELP transmission attempts, the director E_Port (failed director) times out and segments. Go to <a href="#">"MAP 0000: Start MAP"</a> on page 46 to perform hardware fault isolation at the failed director.</p>						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 072							
Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The director is attached (through an ISL) to an incompatible fabric element (director or switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 073							
Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the backup CD to HP Services support personnel.						
Event Data:	Byte 0 = error reason code for engineering evaluation. Byte 1 = reserved. Bytes 4–9 = port numbers for which problems were detected.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (073 event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the backup CD to HP Services support personnel.						
Event Data:	Byte 0 = E_Port number reporting the problem. Byte 1 = reserved.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The worldwide name of the device or director plugged in the indicated port is not authorized for that port.						
Action:	Change the port binding definition or plug the correct device or director into this port.						
Event Data:	Byte 0 = Port number reporting the unauthorized connection. Bytes 1–3 = reserved. Bytes 4–11 = WWN of the unauthorized device or fabric element.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓	✓		✓	

Event Code: 081	
Message:	Invalid attachment.

Severity:	Informational.
Explanation:	A director port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.
Action:	Action depends on the reason specified in the event data.
Event Data:	<p>The first byte of event data (byte 0) specifies the port number. The fifth byte (byte 4) specifies the isolation reason as follows:</p> <p>1 = Unknown–Isolation reason is unknown, but probably caused by failure of a device attached to the director through an E_Port connection. Fault isolate the failed device or contact support personnel to report the problem.</p> <p>2 = ISL connection not allowed–The port connection conflicts with the configured port type. Change the port type to F_Port if the port is cabled to a device, or E_Port if the port is cabled to a fabric element to form an ISL.</p> <p>3 = Incompatible switch–The director returned a Process ELP Reject–Unable to Process reason code because the attached fabric element is not compatible. Set the director operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p>4 = Incompatible switch–The director returned a Process ELP Reject–Invalid Revision Level reason code because the attached fabric element is not compatible. Set the director operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p>5 = Loopback plug connected–A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug.</p> <p>6 = N_Port connection not allowed–The director is connected to a fabric element through a port configured as an F_port. Change the port type to E_Port.</p> <p>7 = Non-HP switch at other end–The attached fabric element is not an HP product. Set the director operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p>A = Unauthorized port binding WWN–The device WWN or nickname used to configure port binding for this port is not valid. Reconfigure the port with the WWN or nickname authorized for the attached device.</p> <p>B = Unresponsive node–The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.</p>

Event Code: 081 (Continued)							
Event Data Continued:	<p>C = ESA security mismatch—Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The fabric binding and director binding parameters for this director and the attached fabric element must agree. Ensure the parameters for both fabric elements are compatible or disable the fabric and director binding features.</p> <p>D = Fabric binding mismatch—Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. Update the fabric membership list for both fabric elements to ensure compatibility or disable the fabric binding feature.</p> <p>E = Authorization failure reject—The fabric element connected to the director through an ISL detected a security violation. As a result, the director received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.</p> <p>F = Unauthorized switch binding WWN—Director binding is enabled and an attached device or fabric element has an incompatible director membership list. Update the director membership list for the director and the attached device or fabric element to ensure compatibility or disable the director binding feature.</p> <p>11 = Fabric mode mismatch—Based on the ELP revision level, a connection was not allowed because an HP switch in legacy mode is attached to an HP switch in Open Fabric mode, or an HP switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch.</p> <p>12 = CNT WAN extension mode mismatch—Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to Computer Network Technologies (CNT) wide area network (WAN) extension mode. Contact Computer Network Technologies for support.</p>						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 090							
Message:	Database replication time out.						
Severity:	Minor						
Explanation:	Replication of a Fabric Services database from master CTP2 to backup has timed out. The backup CTP2 has been dumped and IPLed. After the backup CTP2 completes the IPL, its databases will be brought up to date and replication will resume.						
Action:	Perform a data collection for this switch using the <i>HAFM</i> application, saving the data file to the HAFM appliance backup drive, and return the backup CD to HP support personnel.						
Event Data:	Bytes 0-3: Type of replication operation that timed out.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error Light	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	4	✓	✓	4		

Event Code: 091							
Message:	Database replication discontinued.						
Severity:	Informational						
Explanation:	Replication of Fabric Services databases from master CTP2 to backup has been discontinued because the backup CTP2 has failed or been removed.						
Action:	<p>This event will occur any time the backup CTP2 fails or is removed and does not require any additional action; when the backup CTP2 is recovered/replaced, its databases will be brought up to date and replication will resume.</p> <p>If this event occurs without the backup CTP2 failing or being removed, perform a data collection operation for this switch using the <i>HAFM</i> application, saving the data file to the HAFM appliance backup drive, and return the backup CD to HP support personnel.</p>						
Event Data:	None						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				



Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the director receives a HAFM Management command that violates specified boundary conditions, typically as a result of a network error. The director rejects the command, drops the director-to-HAFM appliance Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection for this director using the <i>HAFM</i> application, save the data file to the HAFM appliance backup drive, and return the backup drive to HP Services support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 121							
Message:	Zone set activation failed—zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the director receives a zone set activation command that exceeds the size supported by the director. The director rejects the command, drops the director-to-HAFM appliance Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 140							
Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 141							
Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 142							
Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 143							
Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 150							
Message:	Zone merge failure.						
Severity:	Informational.						
Explanation:	During ISL initialization, the zone merge process failed. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a 070 ISL segmentation event code, and represents the reply of an adjacent fabric element in response to a zone merge frame. Refer to the event data for the failure reason.						
Action:	Action depends on the failure reason specified in the event data.						

Event Code: 150 (Continued)	
Event Data:	<p>Bytes 0–3 of the event data specify affected E_Port number(s). Bytes 8–11 specify the failure reason as follows:</p> <p>01 = Invalid data length—An invalid data length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p> <p>08 = Invalid zone set format—An invalid zone set format caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p> <p>09 = Invalid data—Invalid data caused a zone merge failure. Inspect bytes 12–15 of the event data for error codes. See the error code definitions on the following page to correct the problem.</p> <p>0A = Cannot merge—A Cannot Merge condition caused a zone merge failure. Inspect bytes 12–15 of the event data for error codes. See the error code definitions on the following page to correct the problem.</p> <p>F0 = Retry limit reached—A retry limit reached condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p> <p>F1 = Invalid response length—An invalid response length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p> <p>F2 = Invalid response code—An invalid response code caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup CD to HP support personnel.</p>

Event Code: 150 (Continued)							
Event Data (Continued):	Bytes 12–15 of the event data specify error codes as follows: 01 = Completion fail. 03 = Zone merge error—too many zones. 04 = Zone merge error—incompatible zones. 05 = Zone merge error—too long if reason = 0A. 06 = Zone set definition too long. 07 = Zone set name too short or not authorized. 08 = Invalid number of zones. 09 = Zone merge error—default zone states incompatible if reason = 0A. 0A = Invalid protocol. 0B = Invalid number of zone members. 0C = Invalid flags. 0D = Invalid zone member information length. 0E = Invalid zone member information format. 0F = Invalid zone member information port. 10 = Invalid zone set name length. 11 = Invalid zone name length. 37 = Invalid zone name. 39 = Duplicate zone. 3C = Invalid number of zone members. 3D = Invalid zone member type. 3E = Invalid zone set name. 45 = Duplicate member in zone. 4A = Invalid number of zones. 4B = Invalid zone set size. 4D = Maximum number of unique zone members exceeded.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓				

## Power Supply Events (200 through 299)

Event Code: 200							
Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	Alternating current (AC) input to the indicated power supply is disconnected or AC circuitry in the power supply failed. The second power supply assumes the full operating load for the director.						
Action:	Ensure the power supply is connected to facility AC power, and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code 203), replace the failed power supply. Perform the data collection procedure and return the backup CD and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 201							
Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	Direct current (DC) circuitry in the power supply failed. The second power supply assumes the full operating load for the director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the backup CD and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 202							
Message:	Power supply thermal failure.						
Severity:	Major.						

Explanation:	The thermal sensor associated with a power supply indicates an overheat condition that shut down the power supply. The second power supply assumes the full operating load for the director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the backup CD and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

### Event Code: 203

Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				



Event Code: 204							
Message:	Power supply DC voltage recovery.						
Severity:	Informational.						
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 206							
Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the director was powered on and operational. The second power supply assumes the full operating load for the director.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 207							
Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the director powered on and operational. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 208							
Message:	Power supply false shutdown.						
Severity:	Major.						
Explanation:	Director operational firmware nearly shut down the indicated power supply as a result of failure or facility power loss or voltage fluctuation.						
Action:	Confirm operation of facility power. If subsequent power loss events occur, replace the failed power supply. Perform the data collection procedure and return the backup CD and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

## Fan Module Events (300 through 399)

Event Code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan (out of six) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan module associated with the failed fan.						
Action:	Replace the indicated fan module.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan number.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 302							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 303							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Four cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of both fan modules.						
Action:	Replace both fan modules						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 304							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Five cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fan is operational. The amber LED illuminates at the rear of both fan modules.						
Action:	Replace both fan modules						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 305							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	All six cooling fans failed or are rotating at insufficient angular velocity. The amber LED illuminates at the rear of both fan modules.						
Action:	Replace both fan modules						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan (out of six) recovered or the associated fan module was replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 311							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans (out of six) recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of six) recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 313							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Four cooling fans (out of six) recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 314							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Five cooling fans (out of six) recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 315							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	All six cooling fans recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				



Event Code: 320							
Message:	Fan module removed.						
Severity:	Major.						
Explanation:	A fan module was removed with the director powered on and operational.						
Action:	Replace the indicated fan module.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓				

Event Code: 321							
Message:	Fan module installed.						
Severity:	Informational.						
Explanation:	A fan module was installed with the director powered on and operational.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

## CTP2 Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a faulty field-replaceable unit (FRU) as indicated by the event data.						
Action:	Replace the failed FRU with a functional FRU. Perform the data collection procedure and return the backup CD and faulty FRU to HP support personnel.						
Event Data:	Byte 0 = FRU code as follows: 01 = backplane, 02 = CTP2 card, 03 = SBAR assembly, 05 = fan module, 06 = power supply, and 08 through 0F = UPM cards. Byte 1 = FRU slot number.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 410							
Message:	CTP2 card reset.						
Severity:	Informational.						
Explanation:	The indicated CTP2 card reset after a director power-on, CTP2 card installation, hardware IML (CTP2 card faceplate), or software IPL. An IPL can be user-initiated at the Element Manager, or occur automatically after a firmware fault (event code 411). The event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte 0 = reset type as follows: 00 = power-on hot-insert, 02 = IML, 04 = IPL, 08 = reset by other CTP2 card, 40 = partition switch, or 80 = dual CTP2 card hot-insert.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 411							
Message:	Firmware fault.						
Severity:	Major.						
Explanation:	<p>Firmware executing on the indicated CTP2 card encountered an unexpected operating condition and dumped the operating state to FLASH memory for retrieval and analysis. The dump file is automatically transferred from the director to the HAFM appliance, where it is stored for retrieval through the data collection procedure.</p> <p>A non-disruptive failover to the backup CTP2 card occurs. When the dump and subsequent IPL complete, the faulty CTP2 card reinitializes to become a the backup.</p>						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	Bytes 0 through 3 = fault identifier, least significant byte first.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 412							
Message:	CTP2 watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP2 card to reset.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	Byte 0 = reset type as follows: 00 = task switch did not occur within approximately one second, 01 = interrupt servicing blocked for more than approximately one second.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 413							
Message:	Backup CTP2 card POST failure.						
Severity:	Major.						
Explanation:	A backup CTP2 card was installed in the director and failed POSTs.						
Action:	Replace the indicated CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 414							
Message:	Backup CTP2 card failure.						
Severity:	Major.						
Explanation:	The backup CTP2 card failed.						
Action:	Replace the indicated CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 415							
Message:	Backup CTP2 card removed.						
Severity:	Informational.						
Explanation:	The backup CTP2 card was removed while the director was powered on and operational.						
Action:	No action required or install an operational backup CTP2 card.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 416							
Message:	Backup CTP2 card installed.						
Severity:	Informational.						
Explanation:	A backup CTP2 card was installed while the director was powered on and operational.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 417							
Message:	CTP2 card firmware synchronization initiated.						
Severity:	Informational.						
Explanation:	The active CTP2 card initiated a firmware synchronization with the backup CTP2 card.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 418							
Message:	User-initiated CTP2 card switchover.						
Severity:	Informational.						
Explanation:	The backup CTP2 card became the active CTP2 card after a user-initiated switchover. The previously active CTP2 card is now the backup CTP2 card.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 420							
Message:	Backup CTP2 card non-volatile memory failure.						
Severity:	Major.						
Explanation:	The backup CTP2 card detected a non-volatile memory failure. The failure has no impact on the active CTP2 card.						
Action:	Replace the indicated CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	Byte 0 = non-volatile memory area identifier.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A director firmware version was downloaded from the HAFM appliance or Embedded Web Server interface. The event data indicates the firmware version in hexadecimal format <i>xx.yy.zz bbbb</i> , where <i>xx</i> is the release level, <i>yy</i> is the maintenance level, <i>zz</i> is the interim release level, and <i>bbbb</i> is the build ID.						
Action:	No action required.						
Event Data:	Bytes 0 and 1 = release level (xx). Byte 2 = always a period. Bytes 3 and 4 = maintenance level (yy). Byte 5 = always a period. Bytes 6 and 7 = interim release level (zz). Byte 8 = always a space. Bytes 9–12 = build ID (bbbb).						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 422							
Message:	CTP2 firmware synchronization complete.						
Severity:	Informational.						
Explanation:	Active CTP2 card synchronization with the backup CTP2 card complete.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 423							
Message:	CTP2 firmware download initiated.						
Severity:	Informational.						



Explanation:	The HAFM appliance initiated download of a new firmware version to the director.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

### Event Code: 426

Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a 426 event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte 0 of the event data (equal to 5, 10, 15, or 20) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to 10 indicates 1,024 ECC error interrupts.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 430							
Message:	Excessive Ethernet transmit errors.						
Severity:	Informational.						
Explanation:	Transmit error counters for the active CTP2 card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP2 card failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.						
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.						
Event Data:	<p>Bytes 0 through 3 = sum of all transmit errors (total_xmit_error).</p> <p>Bytes 4 through 7 = frame count where Ethernet adapter does not detect carrier sense at preamble end (loss_of_CRSSs_cnt).</p> <p>Bytes 8 through 11 = frame count where Ethernet adapter does not detect a collision within 64 bit times at transmission end (SQE_error_cnt).</p> <p>Bytes 12 through 15 = frame count where Ethernet adapter detects a collision more than 512 bit times after first preamble bit (out_of_window_cnt). Frame not transmitted.</p> <p>Bytes 16 through 19 = frame count where transmission is more than 26 ms (jabber_cnt). Frame not transmitted.</p> <p>Bytes 20 through 23 = frame count where Ethernet adapter encounters 16 collisions while attempting to transmit a frame (16coll_cnt). Frame not transmitted.</p>						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 431							
Message:	Excessive Ethernet receive errors.						
Severity:	Informational.						
Explanation:	Receive error counters for the active CTP2 card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP2 card failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.						
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.						
Event Data:	<p>Bytes 0 through 3 = sum of all receive errors (total_rcv_error).</p> <p>Bytes 4 through 7 = frame count where received frame had from 1 to 7 bits after last received full byte (dribble_bits_cnt). CRC error counter updated but frame not processed.</p> <p>Bytes 8 through 11 = frame count where received frame had bad CRC (CRC_error_cnt). Frame not processed.</p> <p>Bytes 12 through 15 = frame count received with less than 64 bytes (runt_cnt). Broadcast frames count but do not contribute to threshold. Frame not processed.</p> <p>Bytes 16 through 19 = frame count received with more than 1518 bytes (extra_data_cnt). Broadcast frames count but do not contribute to threshold. Frame not processed.</p>						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 432							
Message:	Ethernet adapter reset.						
Severity:	Minor.						
Explanation:	The active CTP2 card Ethernet adapter was reset in response to an internally detected error. A card failure is not indicated. The director-to-HAFM appliance connection terminates, but automatically recovers after the reset.						
Action:	Perform the data collection procedure and return the backup CD to HP support personnel.						
Event Data:	Bytes 0 through 3 = reason for adapter reset, least significant byte first (reset_error_type) 1 = completion notification for timed-out frame transmission.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 433							
Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A nonrecoverable error was detected on the CTP2 card Ethernet adapter and the LAN connection to the HAFM appliance or Internet terminated. All Fibre Channel switching functions remain unaffected. This event only occurs on a director with a single CTP2 card. Because Ethernet communication is lost, no failure indication is externally reported.						
Action:	Replace the CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP Services support personnel.						
Event Data:	Byte 0 = LAN error type, where 01 = hard failure and 04 = registered fault. Byte 1 = LAN error subtype (internally defined). Byte 2 = LAN fault identifier (internally defined).						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal CTP2 card error.						
Action:	Replace the indicated CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	Byte 0 = CTP2 slot position (00 or 01). Byte 1 = engineering reason code Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP2 card detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte 0 = port number. Byte 1 = engineering reason code.port. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Byte 14 = participating SBAR assembly. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 450							
Message:	Serial number mismatch detected.						
Severity:	Informational						
Explanation:	This event occurs when the sequence number or OEM serial number in the system VPD (read from the backplane) does not match the sequence number and serial number that were saved in NVRAM the last time the switch was IPLed. This event will occur normally when a CTP2 is moved from one switch to the master position of another switch. This event may occur abnormally when a hardware problem is causing a problem reading the system VPD from the backplane.						
Action:	None. Any configured feature keys will be cleared, configuration information will be synched with the backplane VPD, and the CTP2 will automatically be IPLed.						
Event Data:	Bytes 0-12 are the sequence number from the system VPD. Bytes 13-31 are the OEM serial number obtained from the system VPD.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 451							
Message:	Switch speed incompatibility detected.						
Severity:	Informational						
Explanation:	The event occurs when the configured switch speed saved in NVRAM conflicts with the speed capability of the switch. This event may occur when backup CTP2 hardware running an early version of software (below 1.3) is improperly synchronized with a CTP2 operating at greater than 1Gb/s.						
Action:	None. Switch speed configuration and port speed configuration data will be set to a level that is compatible with the CTP2 and the CTP2 will automatically be IPLed.						
Event Data:	None						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 453							
Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the HAFM appliance or Embedded Web Server interface. The director performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.						
Action:	No action required.						
Event Data:	Byte 0 = feature description as follows: 00 through 04 = Flexport, 06 = open-system HAFM appliance. Byte 1 = feature description as follows: 06 = SANtegrity Binding, 07 = Open Trunking.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				



## UPM Card Events (500 through 599)

Event Code: 500							
Message:	UPM card hot-insertion initiated.						
Severity:	Informational						
Explanation:	Installation of a UPM card was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the UPM card, but the card is not seated. When the card is seated in the director chassis and identified by firmware, an event code 501 is generated.						
Action:	If event code 501 follows this event and the amber LED on the UPM card extinguishes, the replacement card is installed and no additional action is required. If event code 501 does not follow this event, re-seat the UPM card. If event code 501 still does not display, replace the UPM card.						
Event Data:	Byte 0 = UPM slot position (00 through 0F). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 501							
Message:	UPM card recognized.						
Severity:	Informational.						
Explanation:	A UPM card is installed and recognized by director operational firmware.						
Action:	No action required.						
Event Data:	Byte 0 = UPM slot position (00 through 0F). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 502							
Message:	UPM card anomaly detected.						

Severity:	Informational.						
Explanation:	The CTP2 card detected a deviation in the normal operating mode or status of the indicated four-port UPM card.						
Action:	No action required. An event code 504 is generated if the UPM card fails.						
Event Data:	Byte 0 = UPM slot position (00 through 0F). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1 Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Byte 14 = participating SBAR assembly. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 503							
Message:	UPM card hot-removal completed.						
Severity:	Informational.						
Explanation:	A UPM card was removed with the director powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = UPM slot position (00 through 0F). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 504							
Message:	UPM card failure.						
Severity:	Major.						
Explanation:	The indicated UPM card failed.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	Byte 0 = UPM slot position (00 through 0F). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 through 11 = reason code specific data.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 505							
Message:	UPM card revision not supported.						
Severity:	Minor.						
Explanation:	The indicated UPM card is not recognized and the four ports display as uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the UPM card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	Byte 0 = UPM slot position (00 through 0F). Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = detected module identifier.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre Channel port on a UPM card failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 through 11 = reason code specific. Byte 16 = connector type. Bytes 17 and 18 = transmitter technology. Byte 19 = distance capabilities. Byte 20 = supported transmission media. Byte 21 = speed capabilities.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code 506 is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 through 11 = reason code specific. Byte 12 = test type.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 508							
Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP2 card detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code 506 is generated if this anomaly results in a hard port failure.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Byte 1 = anomaly reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Byte 14 = participating SBAR assembly. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 509							
Message:	Fibre Channel path failure.						
Severity:	Major.						
Explanation:	<p>One or more of the backplane data paths has been removed from service, thus reducing the bandwidth capabilities of the associated port. This does not prevent the port from frame reception or transmission, but it does limit the potential throughput of the port.</p> <p>Normally the amber Service Required LED on the port associated with the failing path is illuminated to indicate the degraded status. The green port LED may or may not be illuminated based on the status of the link.</p>						
Action:	<p>Replace the port card on which the failed path resides with a functional port (UPM) card of the same type. Perform a data collection operation of this director using the <i>HAFM</i> application, saving the data file to the HAFM appliance Zip drive. Return the failed port card and the data file to the manufacturer for analysis and repair. A failed path may also be recovered by performing a port reset with the <i>HAFM</i> application, however any newly detected errors may cause the path to re-fail.</p>						
Event Data:	<p>Byte 0 = port number (00 through 63).</p> <p>Byte 1 = engineering reason code.</p> <p>Bytes 4 - 7 = elapsed millisecond tick count.</p>						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	



Event Code: 510							
Message:	SFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of a small form factor pluggable (SFP) optical transceiver was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 512							
Message:	SFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Director firmware detected an SFP optical transceiver nonfatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 513							
Message:	SFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An SFP optical transceiver was removed while the director was powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 514							
Message:	SFP optical transceiver failure.						
Severity:	Major.						
Explanation:	An SFP optical transceiver in a UPM card failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (0-127 and 132-143). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 581							
Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">"MAP 0000: Start MAP"</a> on page 46 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

Event Code: 582							
Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">"MAP 0000: Start MAP"</a> on page 46 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">“MAP 0000: Start MAP”</a> on page 46 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server received a not-operational primitive sequence (NOS).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">“MAP 0000: Start MAP”</a> on page 46 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

Event Code: 585							
Message:	Primitive sequence timeout.						

Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was no longer recognized).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">"MAP 0000: Start MAP"</a> on page 46 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

**Event Code: 586**

Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">"MAP 0000: Start MAP"</a> on page 46 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

## SBAR Assembly Events (600 through 699)

Event Code: 600							
Message:	SBAR assembly hot-insertion initiated.						
Severity:	Informational						
Explanation:	Installation of a backup SBAR was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the SBAR, but the SBAR is not seated. When the SBAR is seated in the director chassis and identified by firmware, an event code 601 is generated.						
Action:	If event code 601 follows this event and the amber LED on the SBAR assembly extinguishes, the replacement SBAR assembly is installed and no additional action is required. If event code 601 does not follow this event, re-seat the SBAR assembly. If event code 601 still does not display, replace the SBAR assembly.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 601							
Message:	SBAR assembly recognized.						
Severity:	Informational.						
Explanation:	An SBAR assembly is installed and recognized by director operational firmware.						
Action:	No action required.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 602							
Message:	SBAR assembly anomaly detected.						

Severity:	Informational.						
Explanation:	Director operational firmware detected a deviation in the normal operating mode or operating status of the indicated SBAR assembly.						
Action:	No action required. An event code 604 is generated if the SBAR assembly fails.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Byte 1 = anomaly reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Byte 14 = participating SBAR assembly. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 603							
Message:	SBAR assembly hot-removal completed.						
Severity:	Informational.						
Explanation:	An SBAR assembly was removed with the director powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 604							
Message:	SBAR assembly failure.						
Severity:	Major.						
Explanation:	The indicated SBAR assembly failed. If the active SBAR assembly fails, the backup SBAR takes over operation. If the backup SBAR assembly fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR assembly with a functional assembly. Perform the data collection procedure and return the backup CD and faulty assembly to HP support personnel.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Byte 1 = engineering failure reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 through 11 = event code specific data.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 605							
Message:	SBAR assembly revision not supported.						
Severity:	Minor.						



Explanation:	The indicated SBAR assembly is not recognized and displays as uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the SBAR assembly with a functional assembly. Perform the data collection procedure and return the backup CD and faulty assembly to HP support personnel.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = detected module identifier.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 607							
Message:	Director contains no operational SBAR assemblies.						
Severity:	Severe.						
Explanation:	The director firmware does not recognize an installed SBAR assembly.						
Action:	Install at least one functional SBAR assembly and power-on reset (POR) the director.						
Event Data:	Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 608							
Message:	User initiated SBAR switch-over.						
Severity:	Informational.						
Explanation:	The backup SBAR has become the active SBAR at a user's request. The previously active SBAR is now the backup SBAR.						
Action:	No action required.						
Event Data:	There is no supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

## Thermal Events (800 through 899)

Event Code: 800							
Message:	High temperature warning (UPM card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a UPM card indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 801							
Message:	Critically hot temperature warning (UPM card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a UPM card indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 802							
Message:	UPM card shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	An UPM card failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code 801).						
Action:	Replace the failed UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 805							
Message:	High temperature warning (SBAR assembly thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR assembly indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR assembly with a functional assembly. Perform the data collection procedure and return the backup CD and faulty assembly to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 806							
Message:	Critically hot temperature warning (SBAR assembly thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR assembly indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR assembly with a functional assembly. Perform the data collection procedure and return the backup CD and faulty assembly to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 807							
Message:	SBAR assembly shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	An SBAR assembly failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code 806). If the active SBAR assembly fails, the backup SBAR takes over operation. If the backup SBAR assembly fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR assembly with a functional assembly. Perform the data collection procedure and return the backup CD and faulty assembly to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 810							
Message:	High temperature warning (CTP2 card thermal sensor).						
Severity:	Major.						

Explanation:	The thermal sensor associated with a CTP2 card indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 811							
Message:	Critically hot temperature warning (CTP2 card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP2 card indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 812							
Message:	CTP2 card shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	A CTP2 card failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code 811). If the active CTP2 card fails, the backup card takes over operation. If the backup CTP2 card fails, the active card is not impacted.						
Action:	Replace the failed CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 850							
Message:	System shutdown due to CTP2 card thermal violations.						
Severity:	Severe.						
Explanation:	The director powered off because of excessive thermal violations on the last operational CTP2 card.						
Action:	Replace the failed CTP2 card with a functional card. Perform the data collection procedure and return the backup CD and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	





# Index

10/100 BaseT ethernet hub [20](#)  
10-100 km configuration, port properties  
  dialog box [180](#)

## A

AC filter module  
  removal [255](#)  
applications  
  management services [25](#)  
ASN.1 format [29](#)  
asynchronous RS-232 null modem cable [32](#)  
audience [12](#)  
authorized reseller, HP [17](#)

## B

backing up, director configuration file [218](#)  
backplane  
  removing and replacing [258](#)  
beaconing  
  fault isolation [21](#)  
blocking  
  port [207](#)  
  UPM card [208](#)

## C

call-home notification  
  information, use of [167](#)  
  reporting [30](#)  
channel wrap test, procedure [195](#)  
cleaning fiber-optic components [199](#)  
configuration changes, audit log [167](#)

configuration data  
  managing [218](#)  
configure panel [28](#)  
configure SNMP dialog box [29](#)  
configure switch parameters dialog box [148](#),  
  [151](#)  
console PC, MAP [157](#)  
conventions  
  document [13](#)  
  equipment symbols [14](#)  
  text symbols [13](#)  
CTP2 card  
  removing and replacing [231](#)  
CTP2 cards  
  event codes tables [354](#)  
  firmware, managing [211](#)  
  FLASH memory [197](#)  
  MAP [110](#)  
  NV-RAM, backing up [218](#)  
customer checklist for fault isolation [46](#)

## D

data collection, procedure [197](#)  
default settings, resetting [220](#)  
diagnostic features, software [24](#)  
diagnostic functions, list of [28](#)  
diagnostics  
  embedded web server [27](#)  
  HAFM application [24](#)  
  MAPs [35](#)  
  port diagnostics [170](#)  
  product manager [24](#)

- dialog boxes
  - configure switch parameters [148, 151](#)
- director
  - diagnostic features, software [24](#)
  - displaying information [188](#)
  - element manager
    - messages [292](#)
  - embedded web server [27](#)
  - ethernet link, MAP [95](#)
  - event codes [319](#)
  - event log
    - recording events [319](#)
  - fault isolation [21, 46](#)
  - firmware [27](#)
  - firmware library dialog box [211](#)
  - firmware, release notes [212](#)
  - general description [20](#)
  - illustrated parts breakdown [265](#)
  - IPL procedure [202](#)
  - MAPs [36](#)
  - ports
    - blocking or unblocking [207](#)
    - port list view [173](#)
  - power-off procedure [201](#)
  - power-on procedure [200](#)
  - reset [204](#)
  - setting online or offline [205](#)
  - SNMP traps [29](#)
  - status table [25](#)
- director 2/64
  - See director
- document
  - conventions [13](#)
  - related documentation [12](#)
- DRAM [197](#)

## E

- E\_port segmentation
  - MAP [141](#)
- e\_port segmentation
  - reasons for [180](#)
- electric shock, warning [200](#)

- electrostatic discharge
  - grounding cable [32](#)
  - wrist strap [32](#)
- electrostatic discharge (ESD)
  - information [229](#)
  - repair procedures, caution [166](#)
- element manager
  - messages [292](#)
  - performance view [175](#)
  - port list view [173](#)
- e-mail notification
  - reporting [30](#)
- embedded web appliance
  - ethernet link, MAP [95](#)
- embedded web server [27](#)
  - fault isolation [46](#)
- equipment rack [20](#)
- equipment symbols [14](#)
- ESD
  - FRU replacement instructions [229](#)
  - FRUs, removing and replacing [228](#)
  - grounding point
    - front [229](#)
    - rear [230](#)
  - information [229](#)
  - precaution requirement [231](#)
  - precaution requirements [230](#)
  - repair procedures, caution [166](#)
- ethernet communication link, MAP [95](#)
- ethernet hub
  - verify operation [99](#)
- event codes
  - CTP2 card events [354](#)
  - description [319](#)
  - fan module events [347](#)
  - power supply events [343](#)
  - SBAR assembly [382](#)
  - system events [321](#)
  - thermal events [387](#)
  - UPM card [369](#)
- event logs
  - HAFM appliance [319](#)

- events
  - exporting 170
  - viewing 169
- exporting
  - events 170
- F**
- fabric logout, MAP 141
- fabric manager
  - logs, list of 167
  - MAP 87
  - messages 272, 292
- factory default settings, resetting 220
- failure analysis 198
- fan module
  - removing and replacing 252
- fan module events, event codes tables 347
- fan modules
  - MAP 110
- fault isolation
  - customer checklist 46
  - diagnostics 35
  - logs 167
  - maintenance approach 21
  - MAPs 36
  - SNMP traps 29
- FC-PH 4.3 20
- Fiber Channel link incidents, MAP 118
- fiber-optic cleaning kit 33
- fiber-optic protective plug 31
- fiber-optic wrap plug 31
- fibre channel address, port properties dialog
  - box 179
- Fibre Channel FE MIB 29
- Fibre Channel physical and signalling interface 20
- FICON
  - fibre channel
    - port address, swapping 176
    - port channel wrapping, enabling and disabling 176
  - FICON management style
    - channel wrap tests
      - performing 170
      - procedure 195
    - fibre channel
      - port address, swapping 175
    - port channel wrapping, enabling and disabling 174
    - swapping ports, procedure 196
- field replaceable units
  - See FRUs
- firmware
  - adding version 212
  - deleting version 215
  - determining version 211
  - downloading version 215
  - modifying description 214
  - release notes 212
  - versions, managing 211
- firmware library 211
- FLASH memory 197
- front-accessible FRUs, parts list 266
- FRUs
  - concurrent 230
  - diagnostic features 24
  - ESD information 229
  - ESD precautions 228
  - front-accessible 266
    - parts list 266
  - illustration 265
  - illustrations 265
  - miscellaneous 270
  - nonconcurrent 231
  - rear-accessible 268
    - parts list 268
  - removing and replacing 229
- full-volatility feature

**G**

gateway address, default [36](#)

getting help [17](#)

grounding point

front [229](#)

rear [230](#)

**H**

HAFM appliance

ethernet link, MAP [95](#)

event log [319](#)

name [50](#), [89](#), [94](#), [103](#), [160](#), [162](#), [225](#)

HAFM application

diagnostic features [24](#)

logs, list of [167](#)

MAP [87](#)

messages [272](#)

HAFM server

fault isolation [21](#)

MAP [46](#)

firmware versions, storing [211](#)

MAP [87](#), [157](#)

hardware view

displaying director information [188](#)

hardware, MAP [157](#)

help

online user documentation [28](#)

help, obtaining [17](#)

hexagonal adapter [30](#)

HP

authorized reseller [17](#)

firmware versions [212](#)

home page [212](#)

storage web site [17](#)

technical support [17](#)

hp StorageWorks director 2/64

See director

hp StorageWorks ha-fabric manager appliance

See HAFM appliance

hp StorageWorks ha-fabric manager

application

See HAFM application

HyperTerminal [33](#), [104](#)

**I**

illustrated parts breakdown [265](#)

IML, compared to IPL [202](#)

initial machine load, compared to IPL [202](#)

initial program load, MAP [81](#)

installing software [223](#)

Internet Explorer

version [27](#)

interswitch link

MAP [141](#)

IP address, default [36](#)

IPL

MAP [81](#)

procedure [202](#)

ISL

MAP [141](#)

**L**

LEDs

beaconing [21](#)

UPM card [171](#)

LIN alerts [174](#)

link incident alerts [174](#)

localhost, HAFM appliance name [50](#), [89](#), [94](#),  
[103](#), [160](#), [162](#), [225](#)

logs

exporting [170](#)

list of [167](#)

viewing [169](#)

loopback tests

external [192](#)

internal [189](#)

**M**

- maintenance analysis procedures
  - See MAPs
- maintenance approach [21](#)
- maintenance data, collecting [197](#)
- maintenance functions, list of [28](#)
- management services application
  - description [25](#)
- managing, configuration data [218](#)
- MAPs [35](#), [36](#)
  - definition [21](#)
  - MAP 0000-Start Map [46](#)
  - MAP 0100-Power Distribution Analysis [71](#)
  - MAP 0200-POST or IML Failure Analysis [81](#)
  - MAP 0300-HAFM Appliance Software
    - Problem Determination [87](#)
  - MAP 0400-Loss of HAFM or Web Browser
    - PC Communication [95](#)
  - MAP 0500-FRU Failure Analysis [110](#)
  - MAP 0600-Port Card Failure and Link
    - Incident Analysis [118](#)
  - MAP 0700-Fabric, ISL, and Segmented Port
    - Problem Determination [141](#)
  - MAP 0800-HAFM Appliance or Web
    - Browser PC Hardware Problem
      - Determination [157](#)
  - quick start [37](#)
- messages
  - element manager [292](#)
  - fabric manager [272](#), [292](#)
  - HAFM application [272](#)
- Microsoft Internet Explorer
  - version [27](#)
- monitor panel [28](#)
- multiswitch fabric
  - e\_port segmentation
    - reasons for [180](#)

**N**

- Netscape Navigator
  - version [27](#)
- null modem cable [32](#)
- NV-RAM, backing up [218](#)

**O**

- offline state, setting [206](#)
- online state, setting [205](#)
- online user documentation [28](#)
- operations panel [28](#)

**P**

- part numbers
  - front-accessible FRUs [266](#)
  - miscellaneous FRUs [270](#)
  - rear-accessible FRUs [268](#)
- password, customer
  - default [36](#)
- password, maintenance
  - default [36](#)
- performance statistics
  - Class 2 [176](#), [186](#)
  - Class 3 [177](#), [186](#)
  - error [177](#)
  - errors [185](#)
  - operational [178](#)
  - traffic [178](#), [185](#)
- port card
  - external loopback test [192](#)
  - internal loopback test [189](#)
  - operational states [171](#)
- port list view [173](#)
- port loopback diagnostic tests, fiber-optic wrap plug [31](#)
- port operational states table [171](#)
- port properties dialog box [174](#), [179](#)

## ports

- blocking [207](#)
- diagnostics, performing [170](#)
- operational states, list of [171](#)
- performance statistics [184](#)
- port properties [187](#)
- port technology [182](#), [187](#)
- unblocking [209](#)

## POSTs

- MAP [81](#)

power distribution system MAP [71](#)

## power module assembly

- removing and replacing [255](#)

## power supply

- removing and replacing [245](#)

power supply events, event codes tables [343](#)power-off procedure [201](#)power-on procedure [200](#)power-on self-tests, MAP [81](#)preventive maintenance, cleaning fiber-optic components [199](#)procedural notes [166](#)

## procedures

- blocking ports [207](#)
- data collection [197](#)
- external loopback test [192](#)
- FRU removal [229](#)
- FRU replacement [229](#)
- installing software [223](#)
- internal loopback test [189](#)
- IPL [202](#)
- managing configuration data [218](#)
- managing firmware versions [211](#)
- MAPs [36](#)
- power-off [201](#)
- power-on [200](#)
- reset [204](#)
- setting offline [205](#)
- setting online [205](#)
- unblocking ports [209](#)

- upgrading software [223](#)

ProComm Plus [33](#)

## product manager

- diagnostic features [24](#)
- logs, list of [167](#)
- MAP [87](#)
- MIB variable, modifying [29](#)

protective plug [31](#)**Q**quick start, MAPs [37](#)**R**rack stability, warning [16](#)rear-accessible FRUs, parts list [268](#)related documentation [12](#)

## remove and replace procedures

- See RRP

repair procedures, notes [166](#)reset, director [204](#)

## resetting

- director configuration data [220](#)

## restoring

- director configuration file [219](#)

RFC 1213 [29](#)

## RRPs

- backplane [258](#)
- CTP2 card [231](#)
- fan module [252](#)
- power module assembly [255](#)
- power supply [245](#)
- procedural notes [228](#)
- SBAR assembly [248](#)
- SFP optical transceiver [241](#)
- UPM card [236](#)
- UPM filler blank [244](#)

## RS-232

- null modem cable [32](#)

**S**

## safety

- basic ESD note 228
- electric shock, warning 200
- electrostatic discharge
  - grounding cable with wrist strap 32

## ESD

- information 229
- repair procedures 166
- fiber-optic protective plug 31

## SBAR assembly

- event codes 382
- MAP 110
- removing and replacing 248
- tools 248

## segmentation

- MAP 141

## service

- maintenance and diagnostic functions 27

## setting

- offline state 206
- online state 205

## SFP optical transceivers

- MAP 118
- removing and replacing 241
- tools 241

## small form factor optical transceivers

- See SFP optical transceivers

## SNMP

- trap messages, reporting 29
- traps, list of 29

## software

- diagnostic features 24
- installing 223
- management services application 25
- upgrading 223

## spare parts

- See FRUs

## statistical information, performance view 175

## status table

- director 25

subnet mask, default 36

swapping ports, procedure 196

symbols in text 13

symbols on equipment 14

system events 21

- event codes tables 321

**T**

TCP/IP MIB-II 29

technical support, HP 17

text symbols 13

thermal events, event codes tables 387

## threshold alert

- port properties dialog box 181
- reasons for 181

## tools

- backplane 258
- CTP2 card 232
- fan module 252
- power module assembly 255
- SBAR assembly 248
- SFP optical transceiver 241
- supplied by service personnel 32
- supplied with director 30
- UPM cards 236
- UPM filler blank 244

torque tool 30

**U**

## unblocking

- port 209
- UPM card 209

upgrading software 223

## UPM cards

- blocking 208
- event codes 369
- LEDs 171
- loopback tests, performing 188
- MAP 118
- ports, blocking or unblocking 207
- removing and replacing 236

- tools [236](#)
- unblocking [209](#)
- UPM filler blank
  - removing and replacing [244](#)
  - tools [244](#)

## V

- versions
  - director firmware [27](#)
  - firmware
    - adding [212](#)
    - deleting [215](#)
    - determining [211](#)
    - downloading [215](#)
    - managing [211](#)
    - modifying description [214](#)
- Internet Explorer [27](#)
- Netscape Navigator [27](#)
- Windows operating systems [33](#)
- view panel [28](#)

- viewing
  - events [169](#)
- views
  - performance [175](#)
  - port list [173](#)

## W

- warning
  - rack stability [16](#)
  - symbols on equipment [14](#)
- web sites
  - HP storage [17](#)
- Windows 2000 operating system
  - MAP [87](#)
- Windows operating systems, versions [33](#)
- wrap plug
  - multimode [31](#)
  - singlemode [31](#)
- WWN
  - port properties dialog box [179](#)